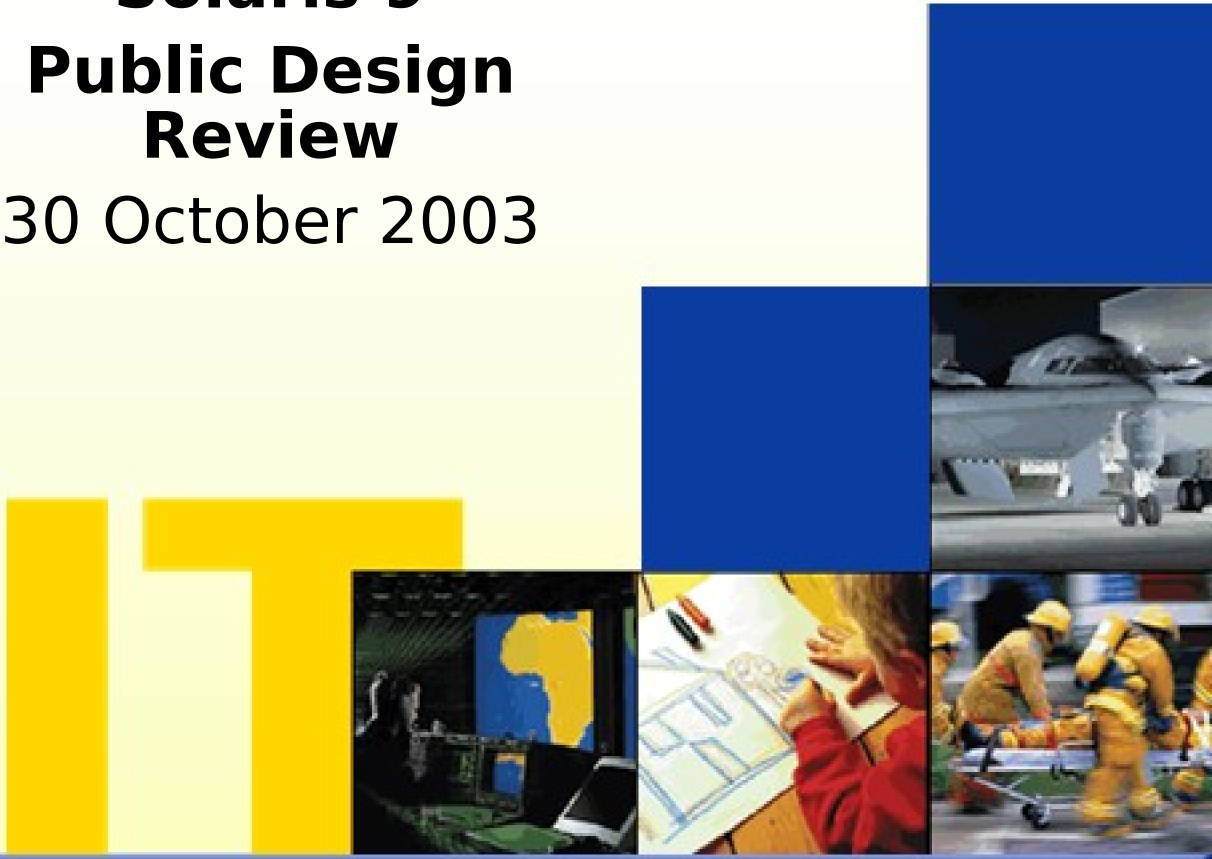
NORTHROP GRUMMAN
Information Technology

JEDI 2.0

Solaris 9

Public Design Review

30 October 2003



Roadmap

- **Solaris 9 Public Design Review**
  - JEDI 2.0 Requirements
  - Support for Solaris 9
  - Transition JEDI Tools to Role Based Access Control
  - Transition JEDI Tools to Solaris Management Console
  - Removing Dependency on JEDI Maps
  - Secure Shell
  - JASS Interface
  - Pluggable Authentication Modules
  - Flash Archive Support
  - Optional SASF for Solaris 9
  - Integration of ISS into JEDI 2.0 Baseline
  - Additional Recommendations

JEDI 2.0 Requirements

- **Support for Solaris 9**
  - JEDI shall
    - Be reengineered to run in the Solaris 9 Operating Environment
  - The Operating Environment shall
    - Be hardened
    - Have a secure file system
    - Use the fix-modes software
    - Use the Solaris fingerprint database
    - Minimize the number of installed accounts
    - Lock unused accounts
    - Start only required services
    - Minimize the required services
    - Minimize the footprint of the system
    - Secure the Solaris Kernel
    - Restrict NFS Server Requests
    - Prevent attempts to execute code on stacks
    - Restrict access to core files

JEDI 2.0 Requirements

- **Transition JEDI tools to Solaris Management Console (SMC)**
  - SMC tools shall
    - Be extended
    - Operate within the SMC framework
    - Conform to the SMC look and feel
    - Have no dependencies
    - Have an associated 16 bit icon
    - Have an associated 32 bit icon
    - Conform to the Sun package standard
    - Conform to existing auditing requirements
    - Support the Graphical SMC Interface
    - Not destroy system data input through other programs

JEDI 2.0 Requirements

- **Transition JEDI tools to Native Role Based Access Control (RBAC)**

- **Remove dependency on JEDI Maps**
  - The JEDI software shall
    - Remove the dependency on the existing JEDI Maps functionality
    - Update operating system files and tables directly
    - Retain the capability to backup and restore name service data

JEDI 2.0 Requirements

- **Integrate Internet Security System's (ISS) Security Scanner**
  - The Security Scanner shall
    - Be included with the JEDI distribution
    - Be installed separately from JEDI
    - Use ISS Installation Scripts
  - Security risks and vulnerabilities shall be documented in the System Security Authorization Agreement (SSAA)
  - Templates shall be documented in the SSAA
  - SPI-NET shall be removed from the JEDI baseline

JEDI 2.0 Requirements

- **Secure Shell**
  - JEDI shall
    - Support secure shell and secure commands
    - Provide a configuration GUI to run the ssh-keygen command
    - Support secure shell on Solaris 8

- **Incorporate new native Pluggable Authentication Modules (PAM)**
  - JEDI shall
    - Incorporate the Solaris 9 native PAM

JEDI 2.0 Requirements

- **Flash Archive Support**

- **Optional Segmented Application Support Framework (SASF) for Solaris 9**
  - JEDI shall
    - Allow for the optional installation of the Segmented Application Support Framework (the DII COE)
    - Provide a version of the DII COE that will run on Solaris 9
    - Use the current version of DII COE and the current patch
    - Support installation of the Integrated C4I System Framework (ICSF) Segments on Solaris 9

JEDI 2.0 Requirements

- **Point and Click Installation**
  - JEDI shall
    - Provide a graphical user interface for installation
    - Provide a consistent look and feel
    - Provide consistent interfaces for Setup, Administration, and DNS
    - Shall support NIS, NIS+, LDAP, and local file installations
    - Shall support Jumpstart Installations

JEDI 2.0 Requirements

- **Solaris 9 Supported Naming Services**
  - JEDI shall support
    - NIS+
    - NIS
    - LDAP/Sun ONE
    - Local Files
    - An upgrade path from JEDI v1.3 on Solaris 8

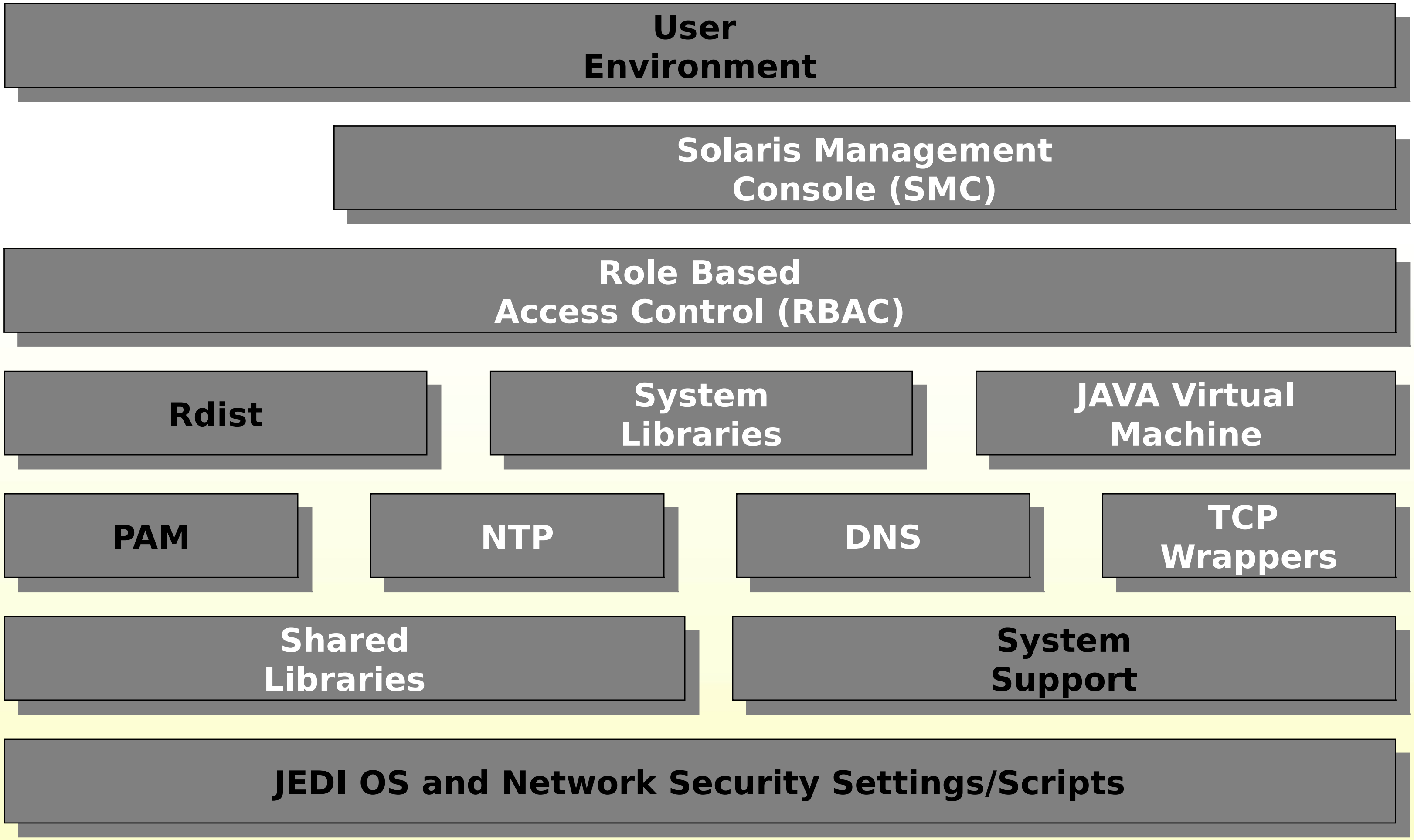
Roadmap

- **Solaris 9 Public Design Review**
  - JEDI 2.0 Requirements
  - ➡ Support for Solaris 9
  - Transition JEDI Tools to Role Based Access Control
  - Transition JEDI Tools to Solaris Management Console
  - Removing Dependency on JEDI Maps
  - Secure Shell
  - JASS Interface
  - Pluggable Authentication Modules
  - Flash Archive Support
  - Optional SASF for Solaris 9
  - Integration of ISS into JEDI 2.0 Baseline
  - Additional Recommendations

Roadmap – Solaris 9

- **Support for Solaris 9**
  - Solaris 9 – Security Architecture
  - Solaris 9 – Security in the Solaris OE
  - Solaris 9 – Solaris Installation Security
  - Solaris 9 – JEDI PreInstallation
  - Solaris 9 – JEDI PostInstallation
  - Solaris 9 – JEDI User Environment
  - Solaris 9 – JEDI/Solaris OE Security

Solaris 9 – Security Architecture



User Environment

Solaris Management Console (SMC)

Role Based Access Control (RBAC)

Rdist

System Libraries

JAVA Virtual Machine

PAM

NTP

DNS

TCP Wrappers

Shared Libraries

System Support

JEDI OS and Network Security Settings/Scripts

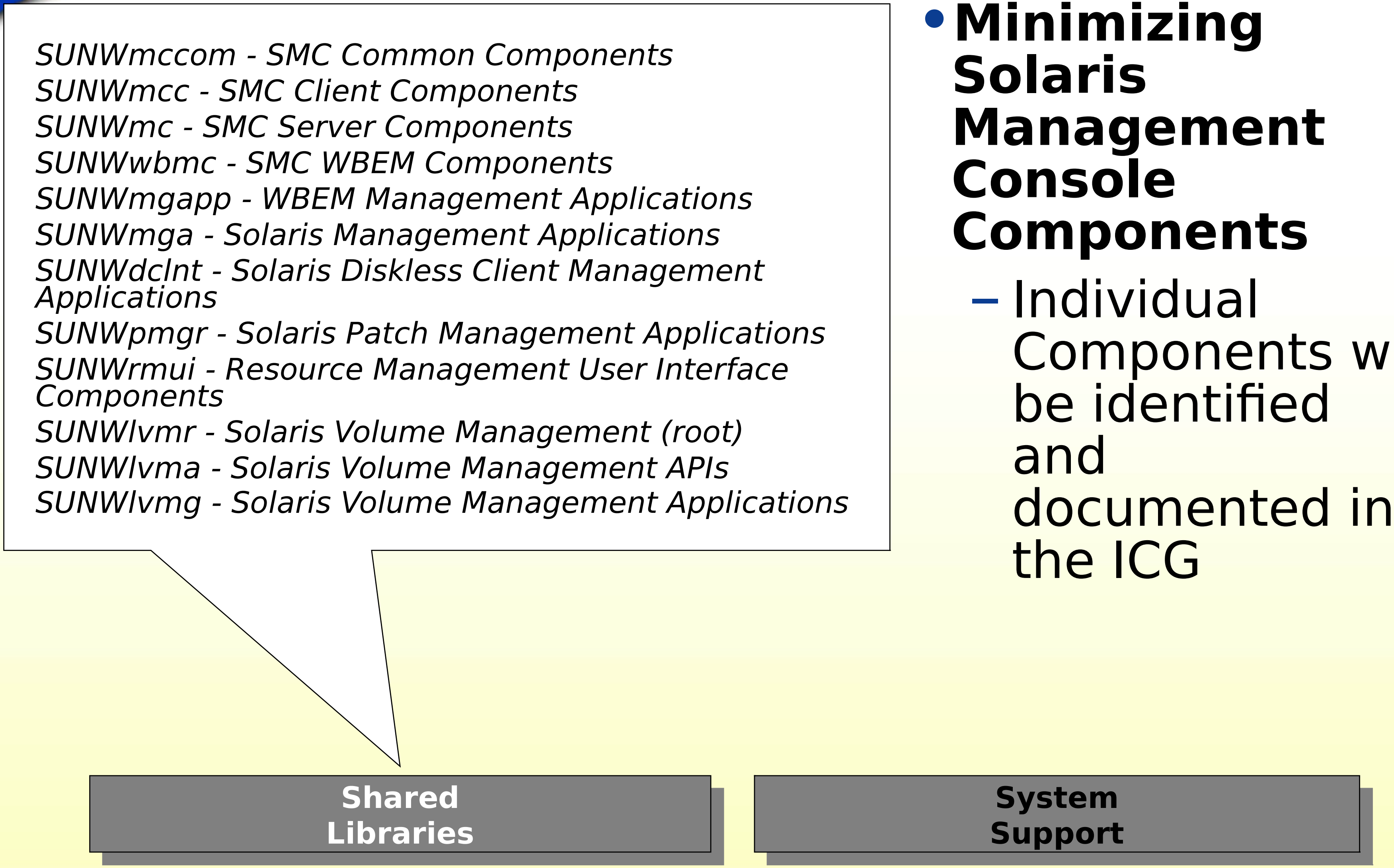
Solaris 9 – Security in the Solaris OE

- **Security will be pervasive in the JEDI Installation**
  - Solaris Installation
  - JEDI PreInstallation
  - JEDI Installation
  - JEDI PostInstallation

Solaris 9 – Solaris Installation Security

- **Software installed as part of Solaris Installation**
  - Minimized Solaris OE Packages
    - User Cluster will be the base
      - Individual Components will be identified and documented in the ICG
    - Solaris Management Console (SMC) Components
    - Dynamic Host Configuration Protocol (DHCP)
  - Secure Shell
  - Jumpstart Architecture and Security Scripts (JASS) Toolkit
    - Fix-modes Software
  - Solaris Fingerprint Database

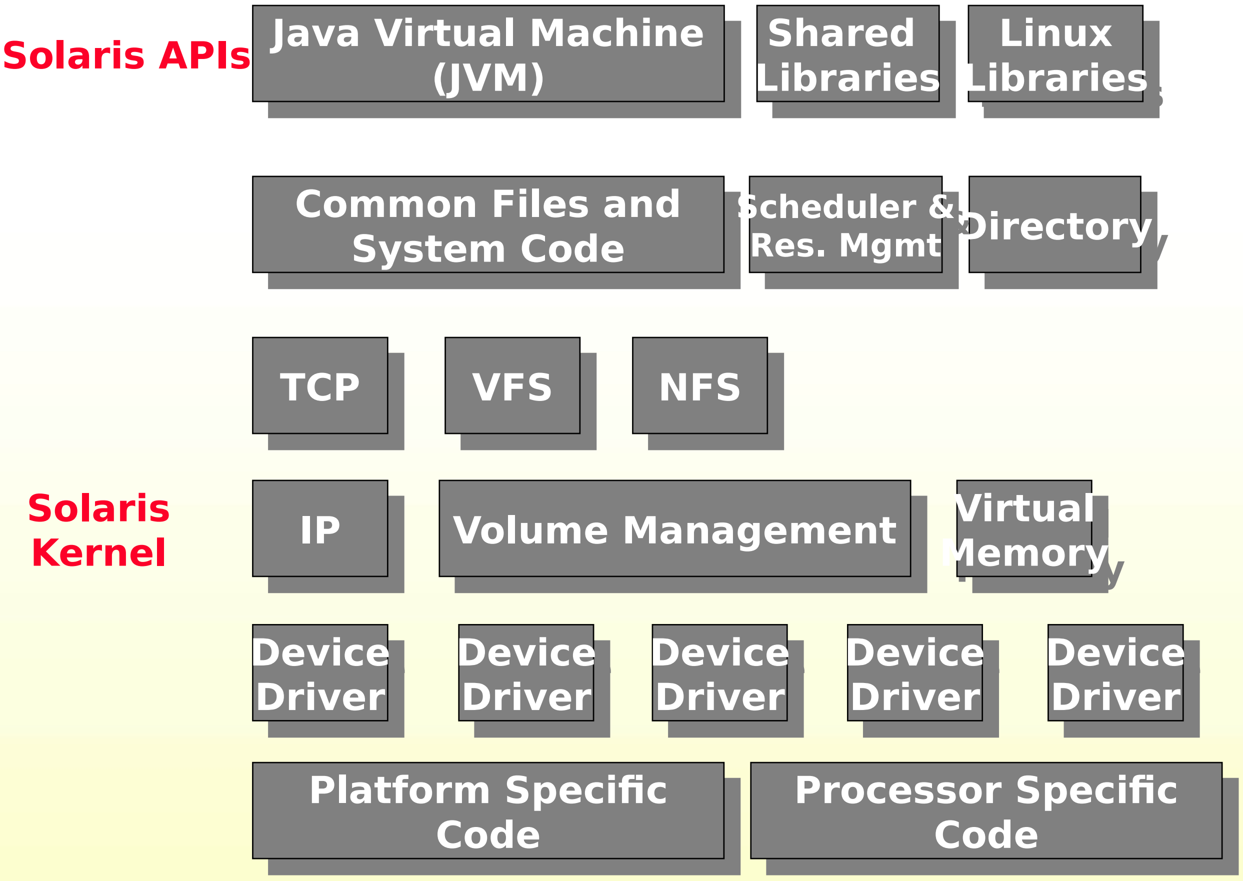
Solaris 9 – Solaris Installation Security



SUNWmccom - SMC Common Components
SUNWmcc - SMC Client Components
SUNWmc - SMC Server Components
SUNWwbmc - SMC WBEM Components
SUNWmgapp - WBEM Management Applications
SUNWmga - Solaris Management Applications
SUNWdclnt - Solaris Diskless Client Management Applications
SUNWpmgr - Solaris Patch Management Applications
SUNWrmui - Resource Management User Interface Components
SUNWlvmr - Solaris Volume Management (root)
SUNWlvma - Solaris Volume Management APIs
SUNWlvmg - Solaris Volume Management Applications

- **Minimizing Solaris Management Console Components**
  - Individual Components will be identified and documented in the ICG

Solaris 9 – Solaris Installation Security



Solaris APIs

Java Virtual Machine (JVM)

Shared Libraries

Linux Libraries

Common Files and System Code

Scheduler & Res. Mgmt

Directory

TCP

VFS

NFS

Solaris Kernel

IP

Volume Management

Virtual Memory

Device Driver

Device Driver

Device Driver

Device Driver

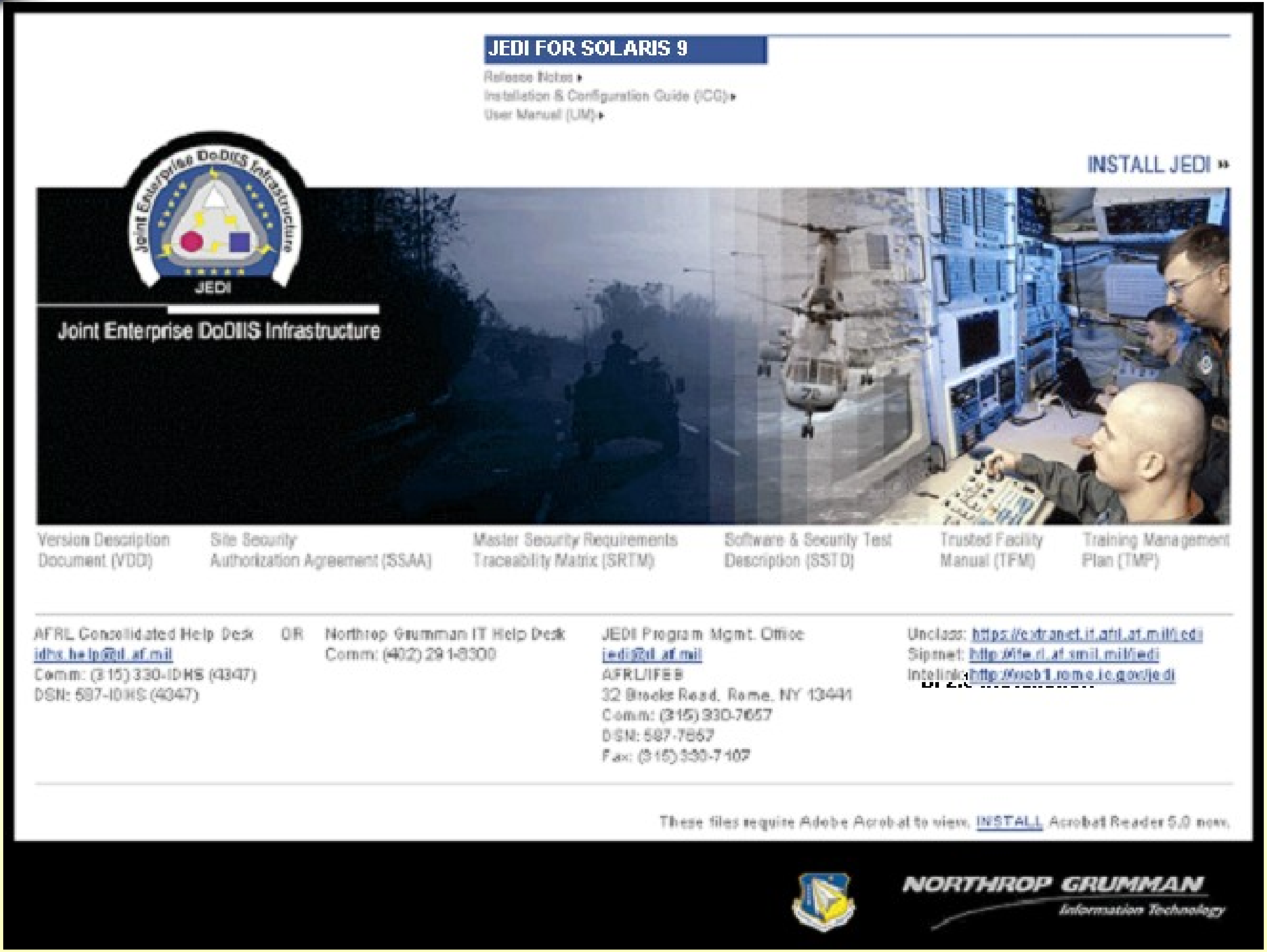
Device Driver

Platform Specific Code

Processor Specific Code

- **Solaris Architecture after Solaris Installation**
  - Modular
  - Highly Configurable
  - Supports multiple architectures

Solaris 9 – JEDI PreInstallation



JEDI FOR SOLARIS 9

Release Notes ▸
Installation & Configuration Guide (ICG) ▸
User Manual (UM) ▸

INSTALL JEDI »

Joint Enterprise DoDIIS Infrastructure

Version Description Document (VDD)
Site Security Authorization Agreement (SSAA)
Master Security Requirements Traceability Matrix (SRTM)
Software & Security Test Description (SSTD)
Trusted Facility Manual (TFM)
Training Management Plan (TMP)

AFRL Consolidated Help Desk
idhs.help@rl.af.mil
Comm: (315) 330-IDHS (4347)
DSN: 587-IDHS (4047)

OR

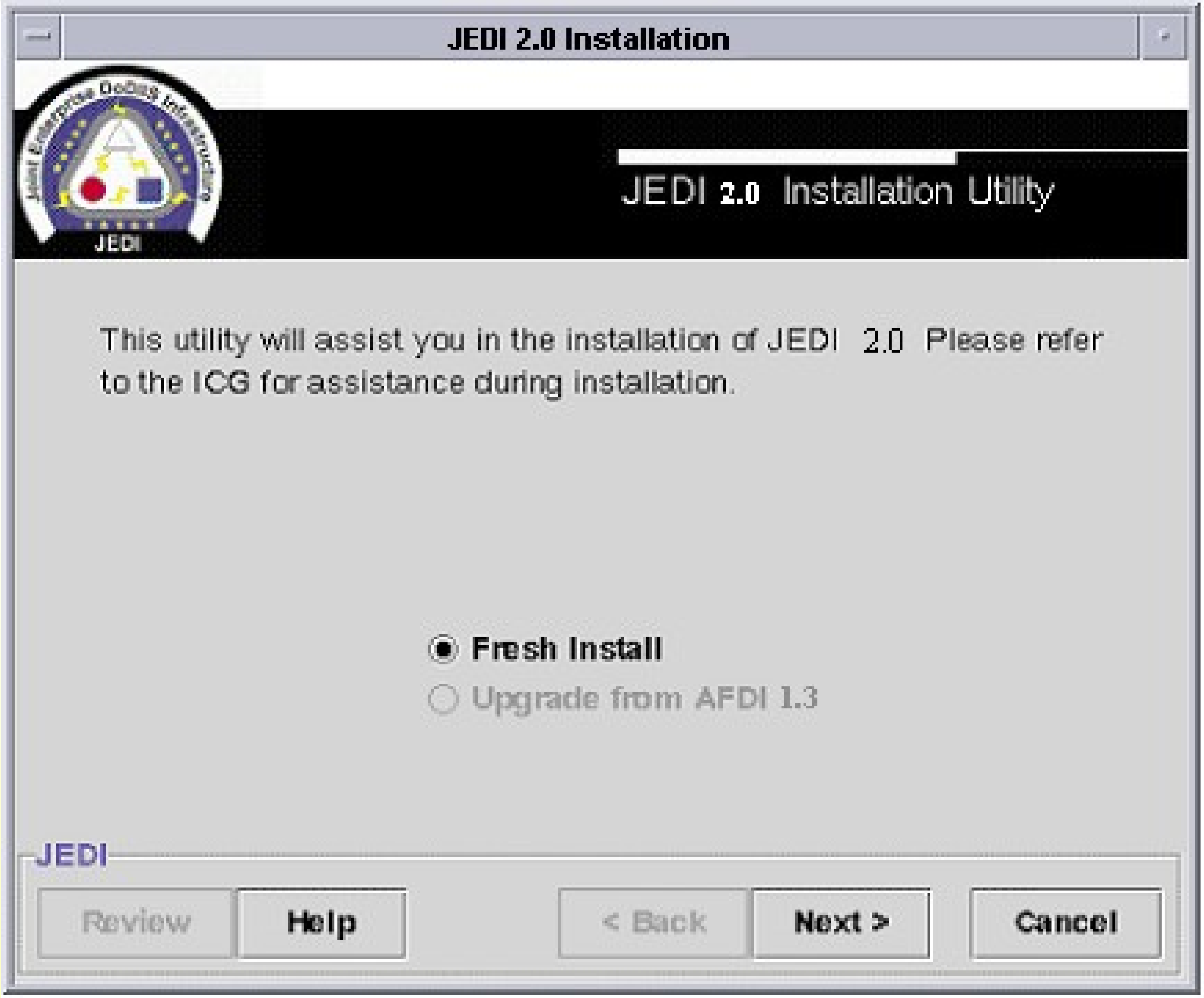
Northrop Grumman IT Help Desk
Comm: (402) 291-8300

JEDI Program Mgmt. Office
jedi@rl.af.mil
AFRL/IFEB
32 Brooks Road, Rome, NY 13441
Comm: (315) 330-7657
DSN: 587-7657
Fax: (315) 330-7107

Unclass: https://extranet.it.afrl.af.mil/jedi
Sipmet: http://ife.rl.af.smil.mil/jedi
Intelink: http://web1.rome.ic.gov/jedi

These files require Adobe Acrobat to view. INSTALL Acrobat Reader 5.0 now.

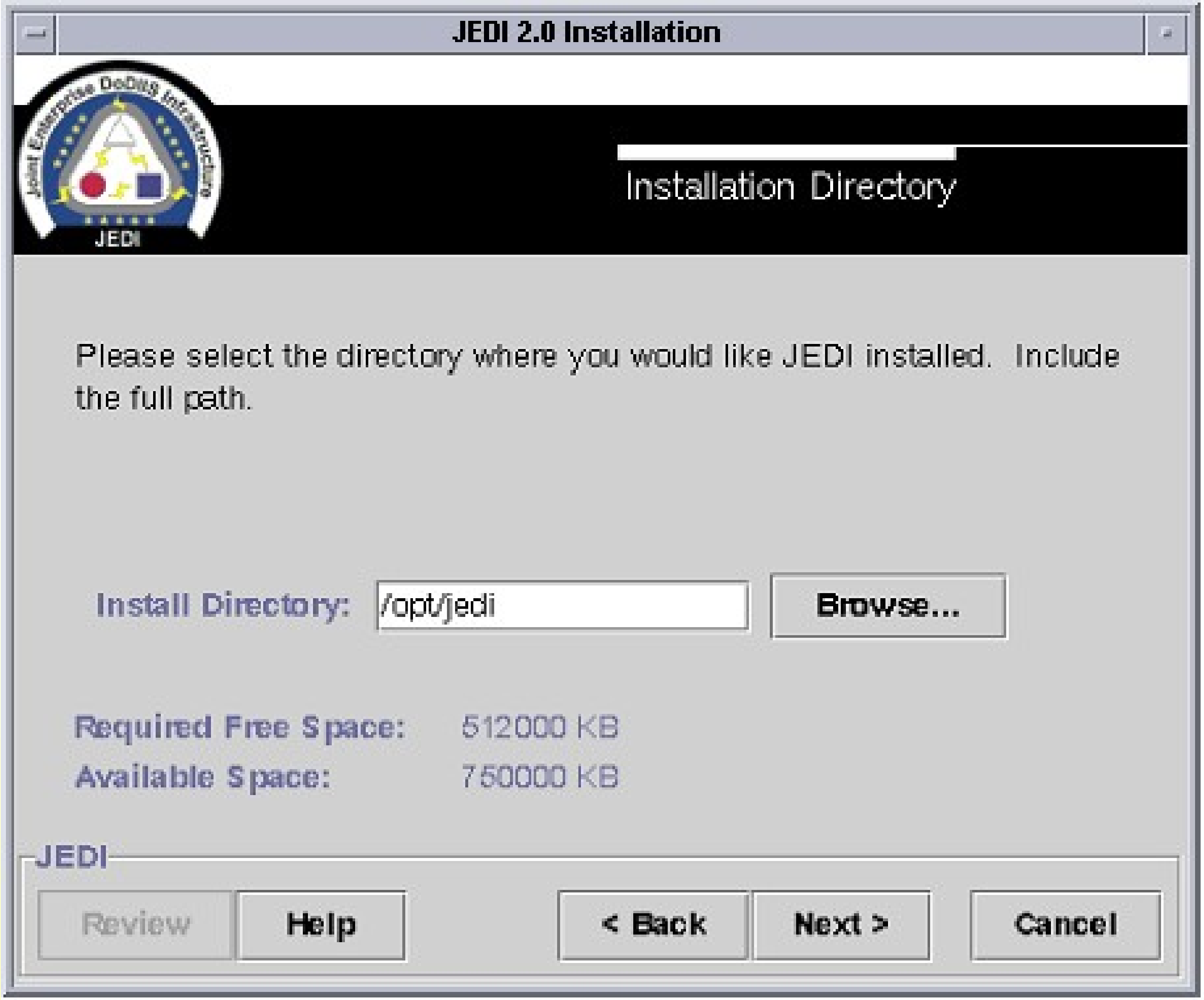
Solaris 9 – JEDI PreInstallation



This utility will assist you in the installation of JEDI 2.0 Please refer to the ICG for assistance during installation.

● Fresh Install
○ Upgrade from AFDI 1.3

Solaris 9 – JEDI PreInstallation



JEDI 2.0 Installation

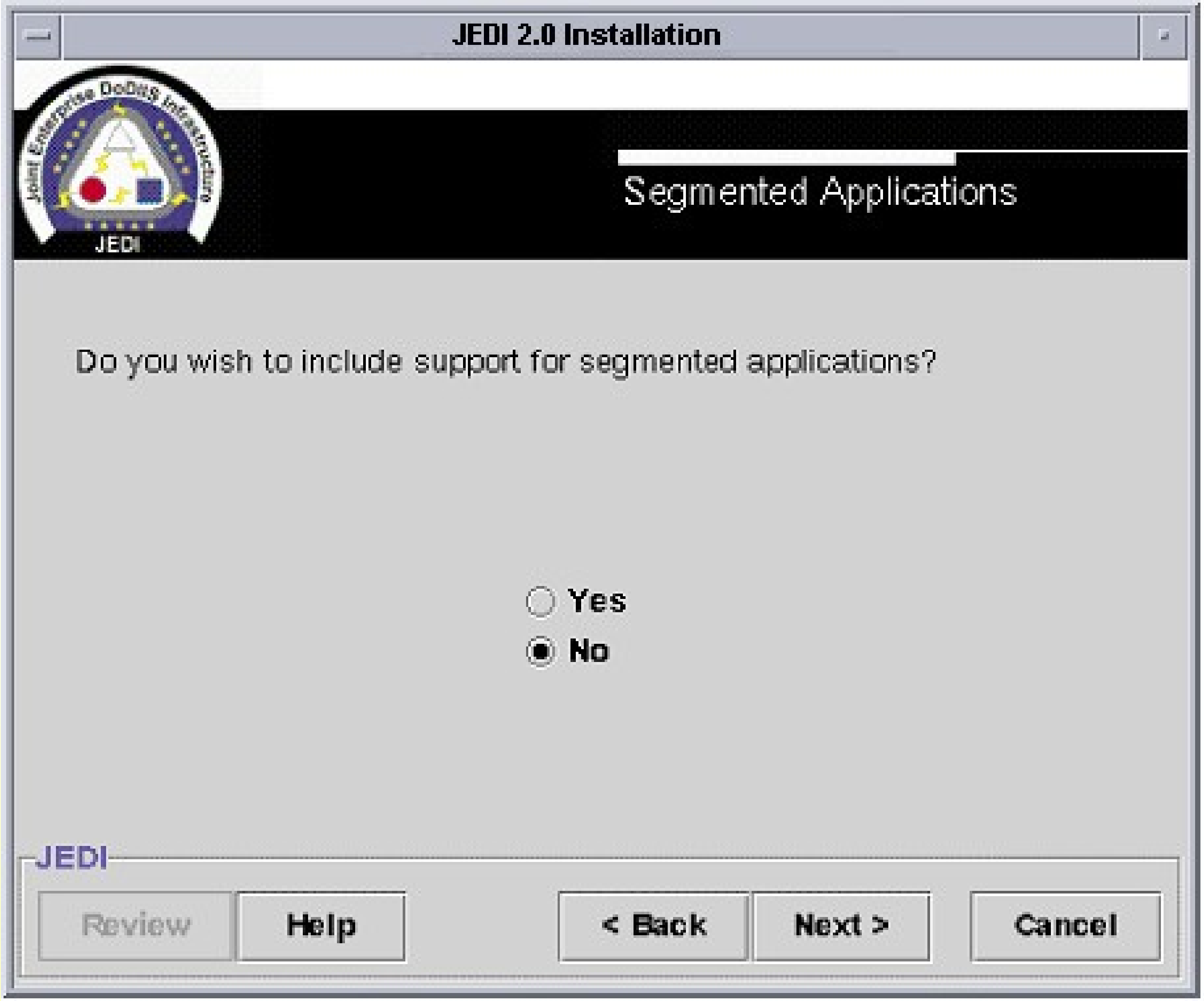
Installation Directory

Please select the directory where you would like JEDI installed. Include the full path.

Install Directory: /opt/jedi

Required Free Space: 512000 KB
Available Space: 750000 KB

Solaris 9 – JEDI PreInstallation



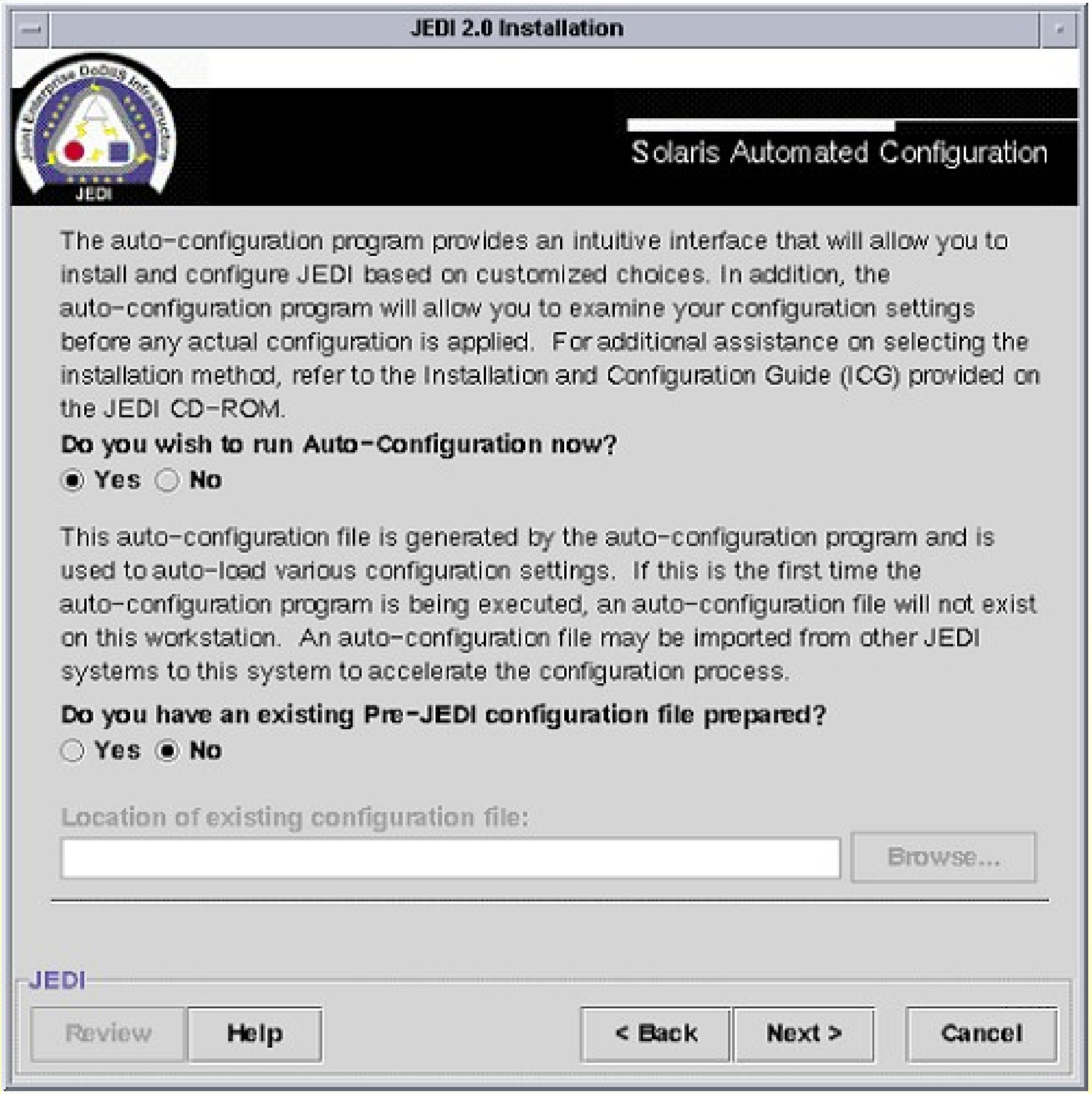
JEDI 2.0 Installation

Segmented Applications

Do you wish to include support for segmented applications?

○ Yes
● No

Solaris 9 – JEDI PreInstallation



JEDI 2.0 Installation
Joint Enterprise DoDIIS Infrastructure
JEDI
Solaris Automated Configuration

The auto-configuration program provides an intuitive interface that will allow you to install and configure JEDI based on customized choices. In addition, the auto-configuration program will allow you to examine your configuration settings before any actual configuration is applied. For additional assistance on selecting the installation method, refer to the Installation and Configuration Guide (ICG) provided on the JEDI CD-ROM.

Do you wish to run Auto-Configuration now?

● Yes ○ No

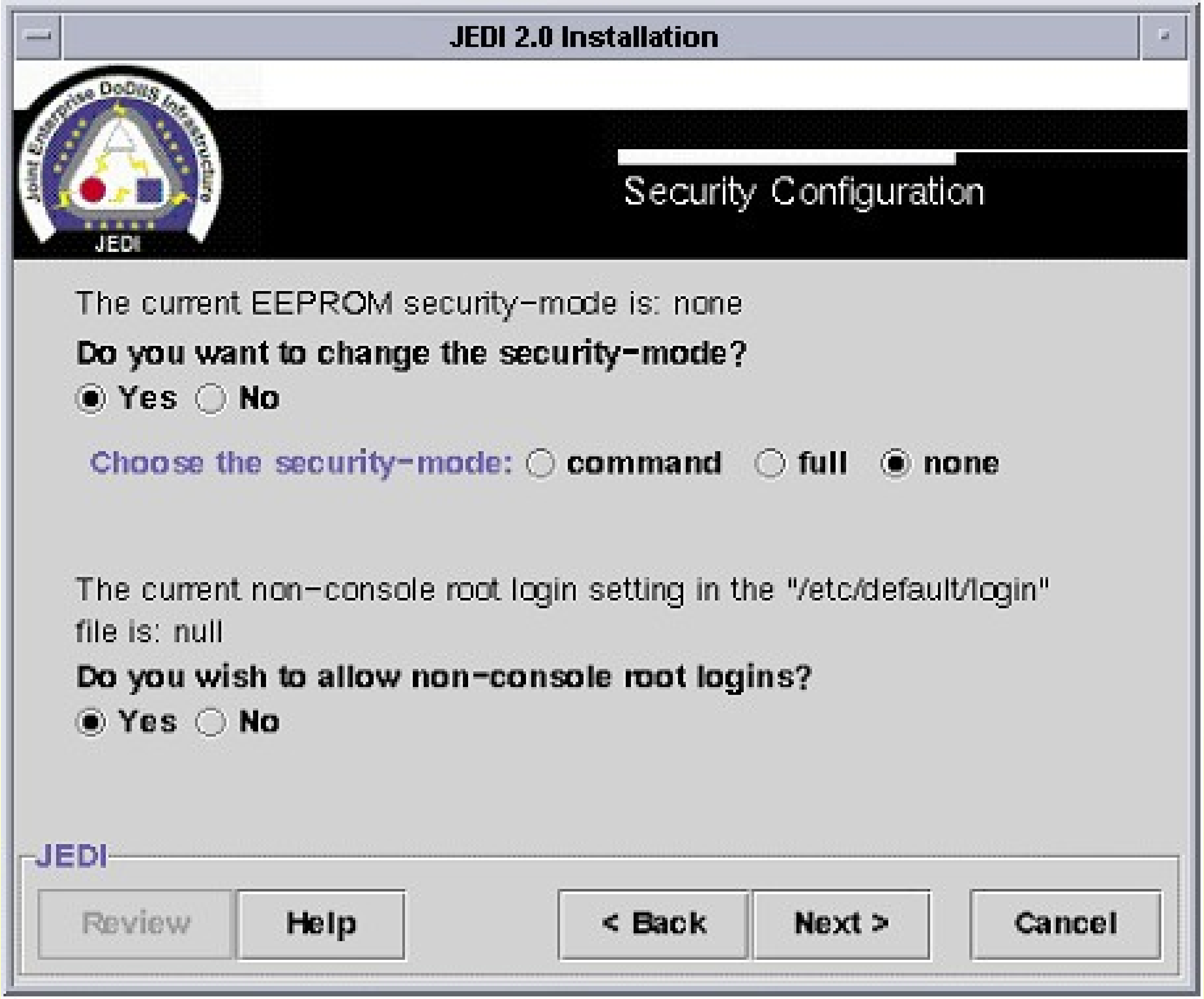
This auto-configuration file is generated by the auto-configuration program and is used to auto-load various configuration settings. If this is the first time the auto-configuration program is being executed, an auto-configuration file will not exist on this workstation. An auto-configuration file may be imported from other JEDI systems to this system to accelerate the configuration process.

Do you have an existing Pre-JEDI configuration file prepared?

○ Yes ● No

Location of existing configuration file:

Solaris 9 – JEDI PreInstallation



Security Configuration

The current EEPROM security-mode is: none

Do you want to change the security-mode?

● Yes ○ No

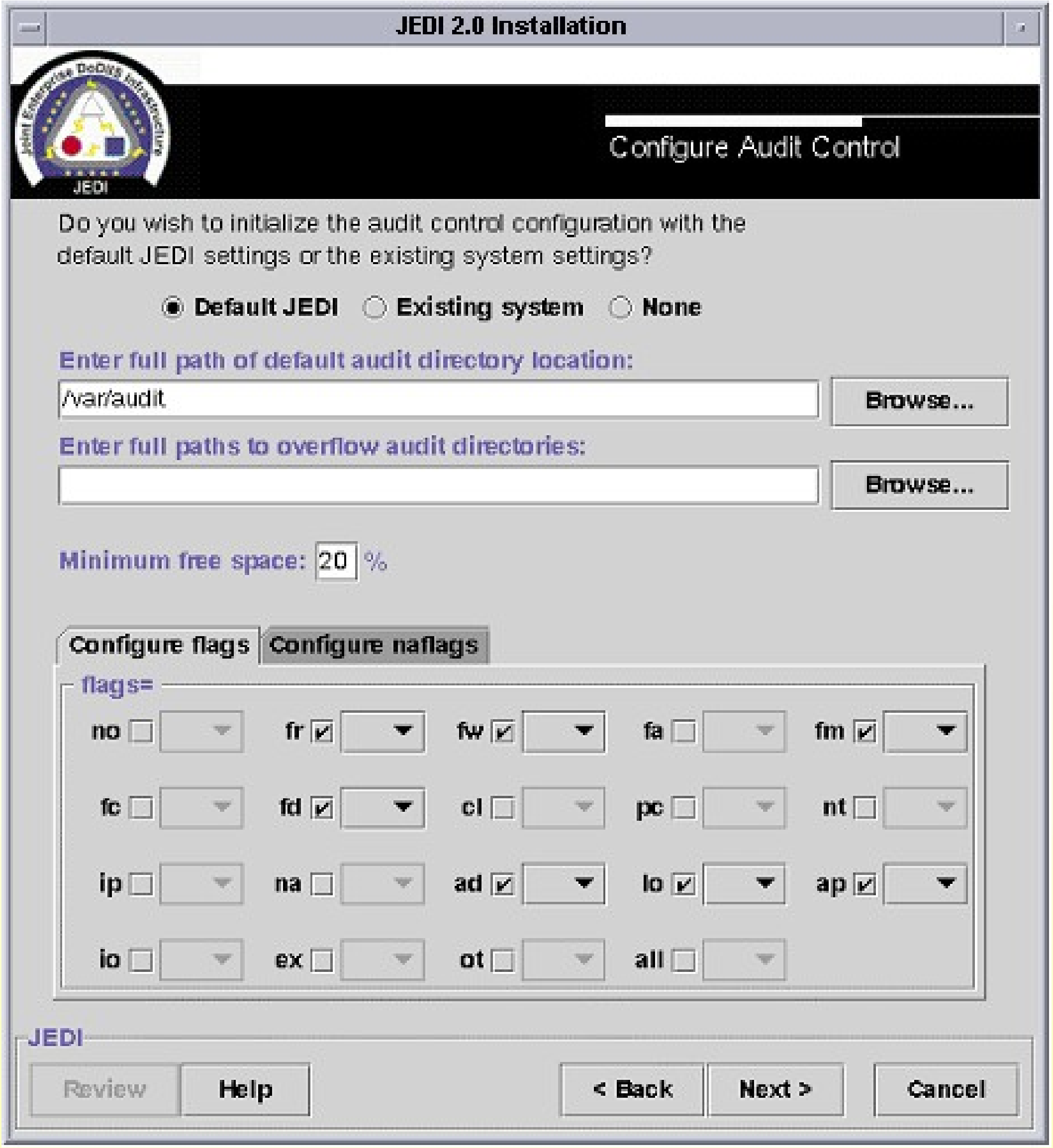
Choose the security-mode: ○ command ○ full ● none

The current non-console root login setting in the "/etc/default/login" file is: null

Do you wish to allow non-console root logins?

● Yes ○ No

Solaris 9 – JEDI PreInstallation



Configure Audit Control

Do you wish to initialize the audit control configuration with the default JEDI settings or the existing system settings?

● Default JEDI ○ Existing system ○ None

Enter full path of default audit directory location: /var/audit

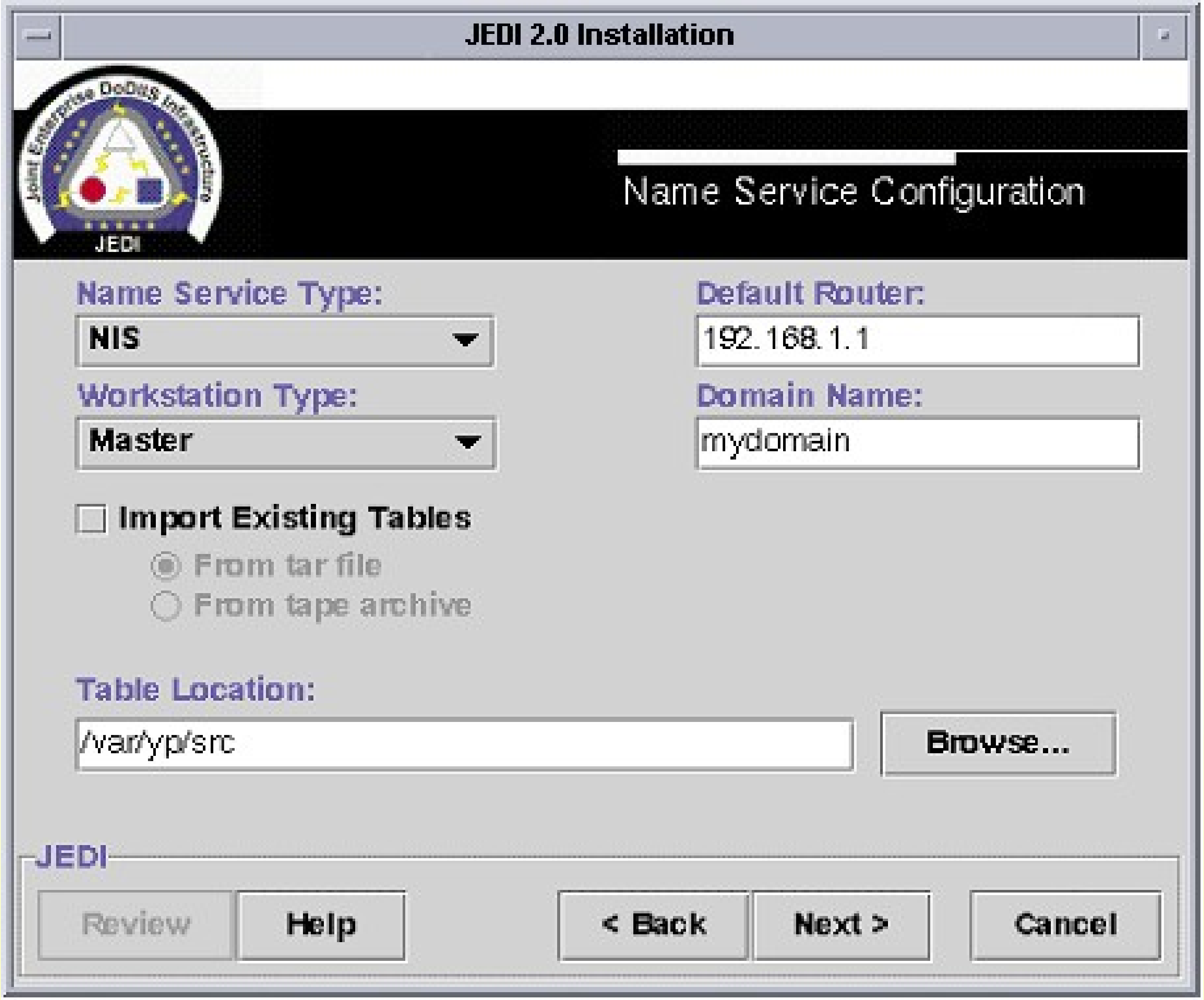
Enter full paths to overflow audit directories:

Minimum free space: 20 %

flags=

no □	fr ☑	fw ☑	fa □	fm ☑
fc □	fd ☑	cl □	pc □	nt □
ip □	na □	ad ☑	lo ☑	ap ☑
io □	ex □	ot □	all □	

Solaris 9 – JEDI PreInstallation



JEDI 2.0 Installation

Name Service Configuration

Name Service Type: NIS

Workstation Type: Master

Default Router: 192.168.1.1

Domain Name: mydomain

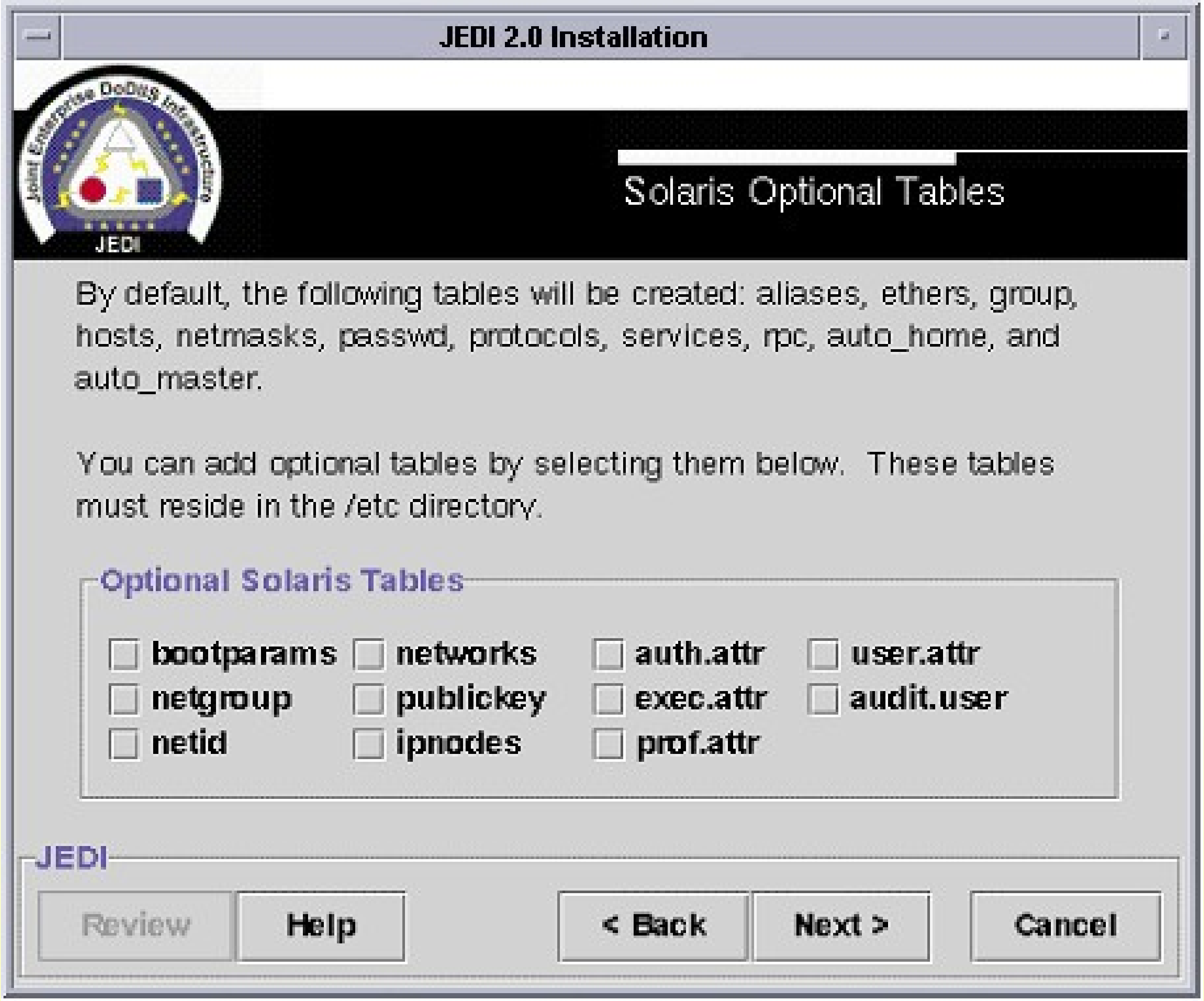
□ Import Existing Tables

● From tar file

○ From tape archive

Table Location: /var/yp/src

Solaris 9 – JEDI PreInstallation



Solaris Optional Tables

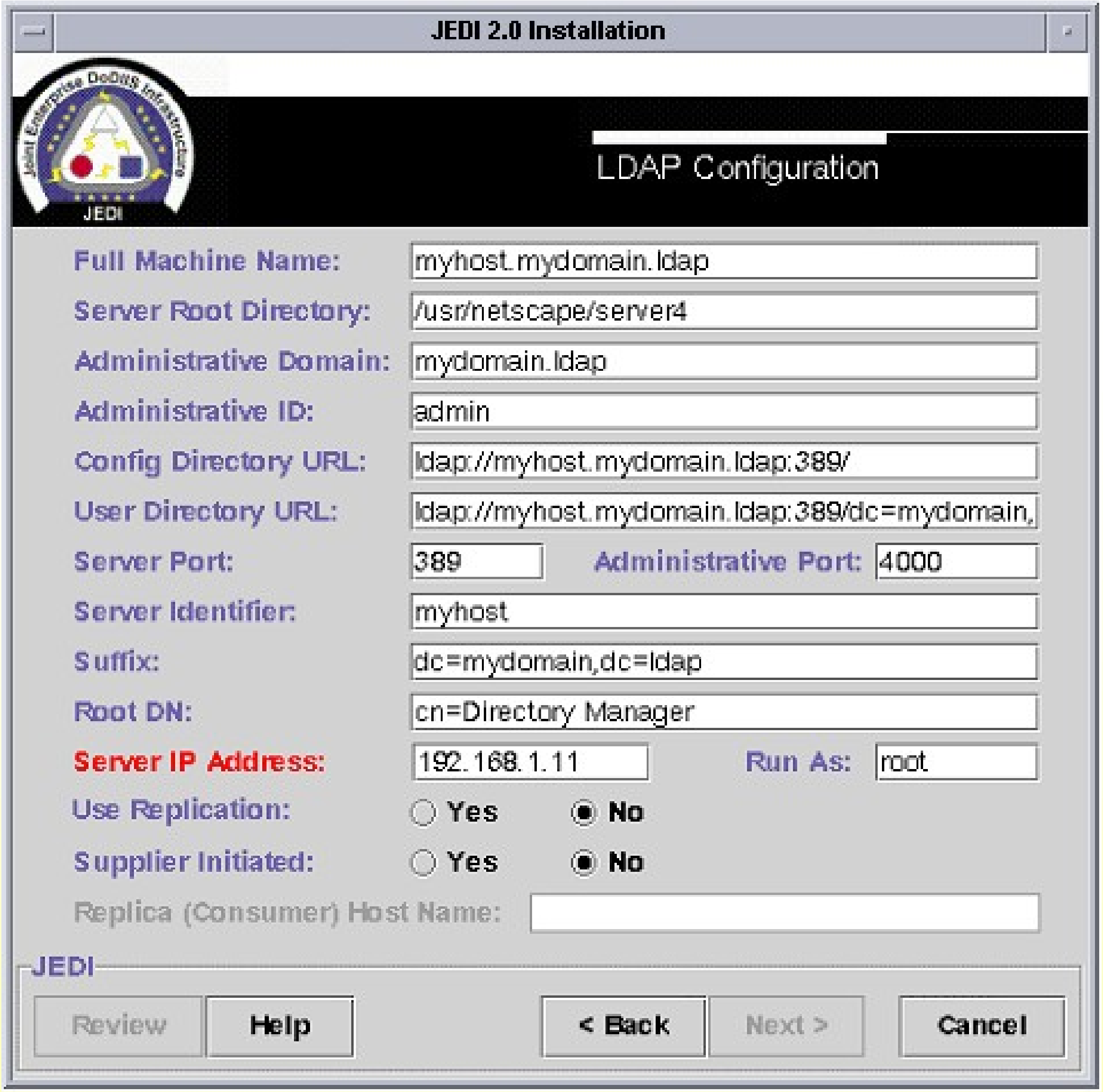
By default, the following tables will be created: aliases, ethers, group, hosts, netmasks, passwd, protocols, services, rpc, auto_home, and auto_master.

You can add optional tables by selecting them below. These tables must reside in the /etc directory.

Optional Solaris Tables

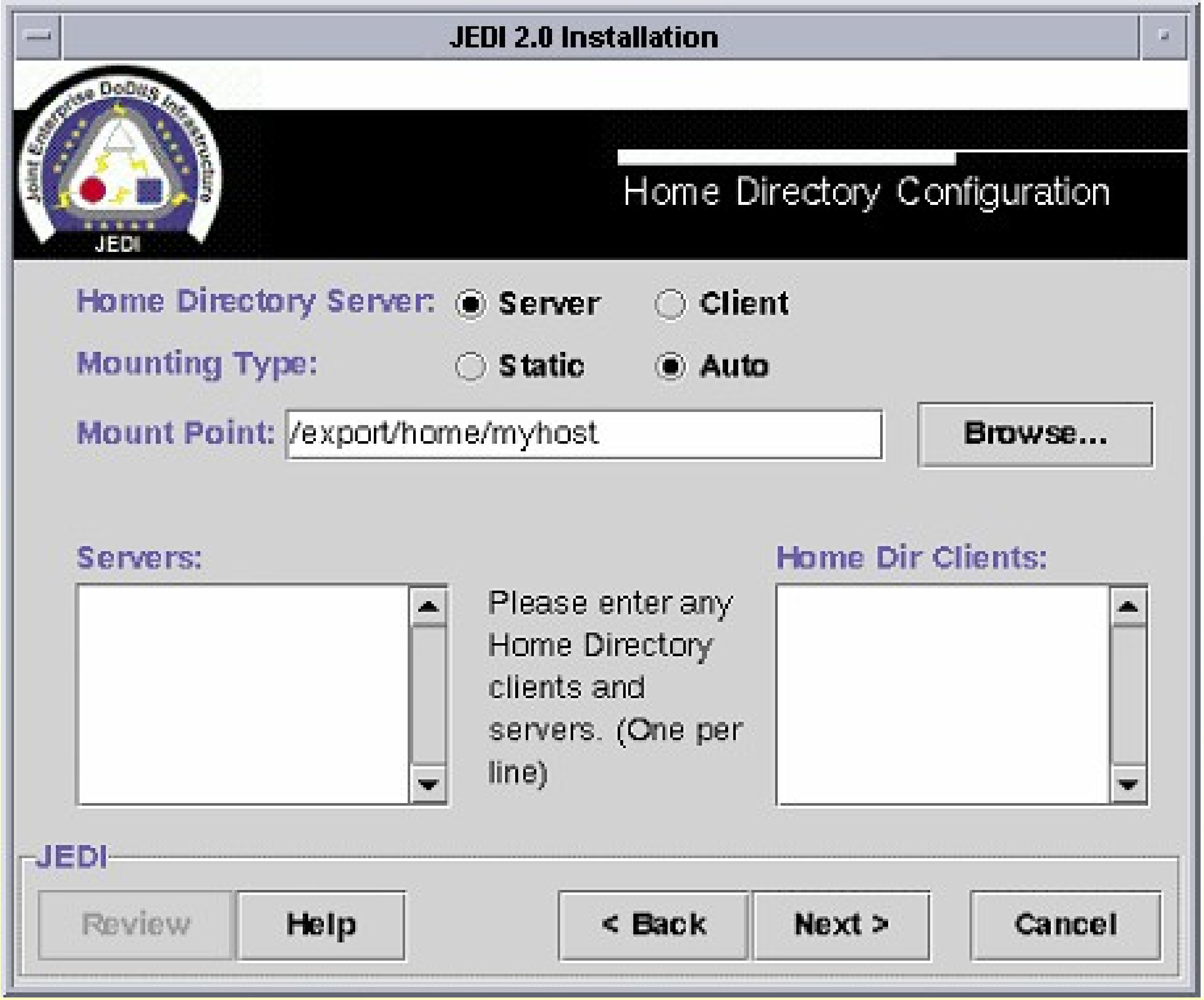
□ bootparams □ networks □ auth.attr □ user.attr
□ netgroup □ publickey □ exec.attr □ audit.user
□ netid □ ipnodes □ prof.attr

Solaris 9 – JEDI PreInstallation



Full Machine Name:	myhost.mydomain.ldap
Server Root Directory:	/usr/netscape/server4
Administrative Domain:	mydomain.ldap
Administrative ID:	admin
Config Directory URL:	ldap://myhost.mydomain.ldap:389/
User Directory URL:	ldap://myhost.mydomain.ldap:389/dc=mydomain,
Server Port:	389
Administrative Port:	4000
Server Identifier:	myhost
Suffix:	dc=mydomain,dc=ldap
Root DN:	cn=Directory Manager
Server IP Address:	192.168.1.11
Run As:	root
Use Replication:	○ Yes ● No
Supplier Initiated:	○ Yes ● No
Replica (Consumer) Host Name:	

Solaris 9 – JEDI PreInstallation



Home Directory Configuration

Home Directory Server: ● Server ○ Client

Mounting Type: ○ Static ● Auto

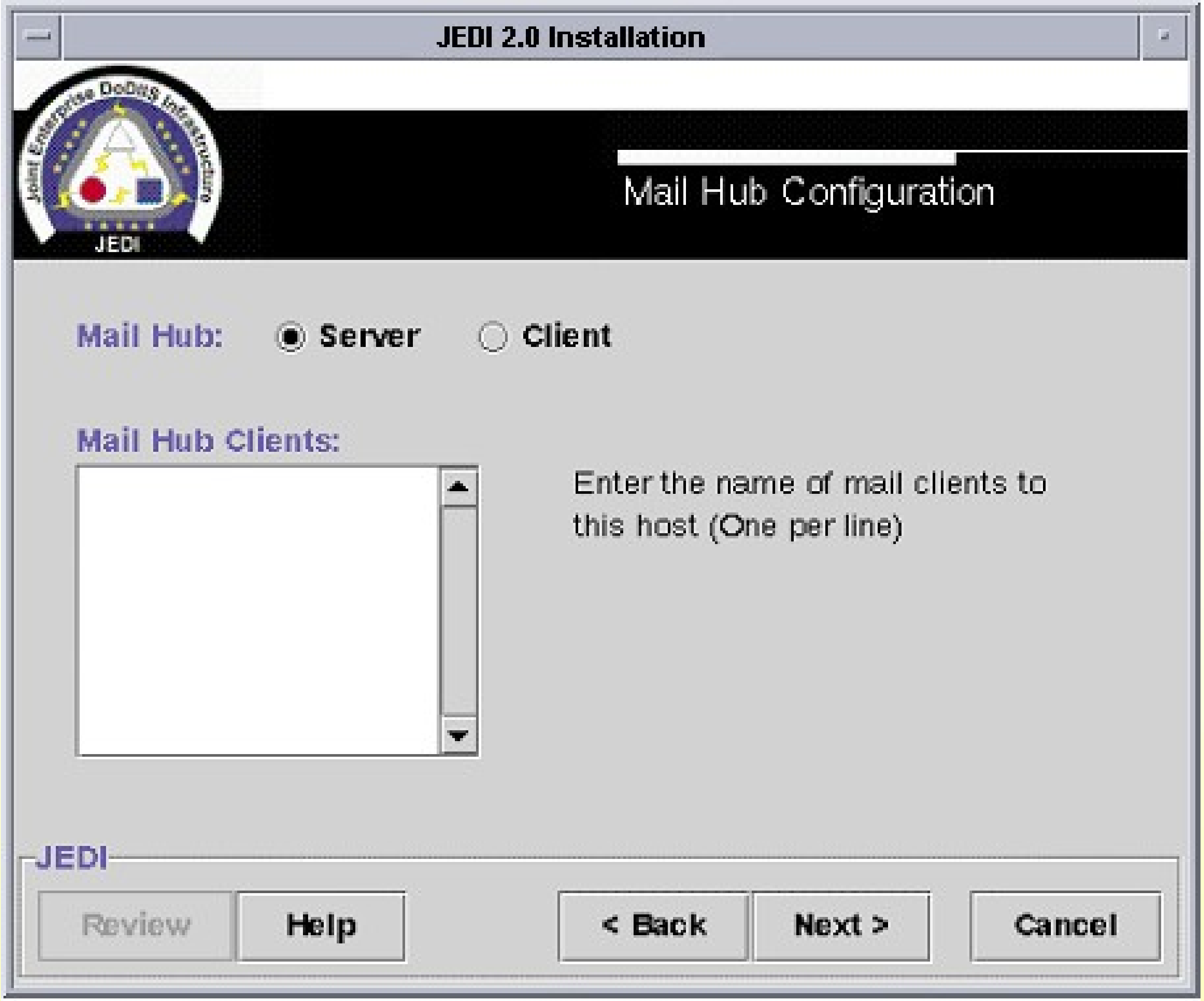
Mount Point: /export/home/myhost

Servers:

Please enter any Home Directory clients and servers. (One per line)

Home Dir Clients:

Solaris 9 – JEDI PreInstallation



JEDI 2.0 Installation

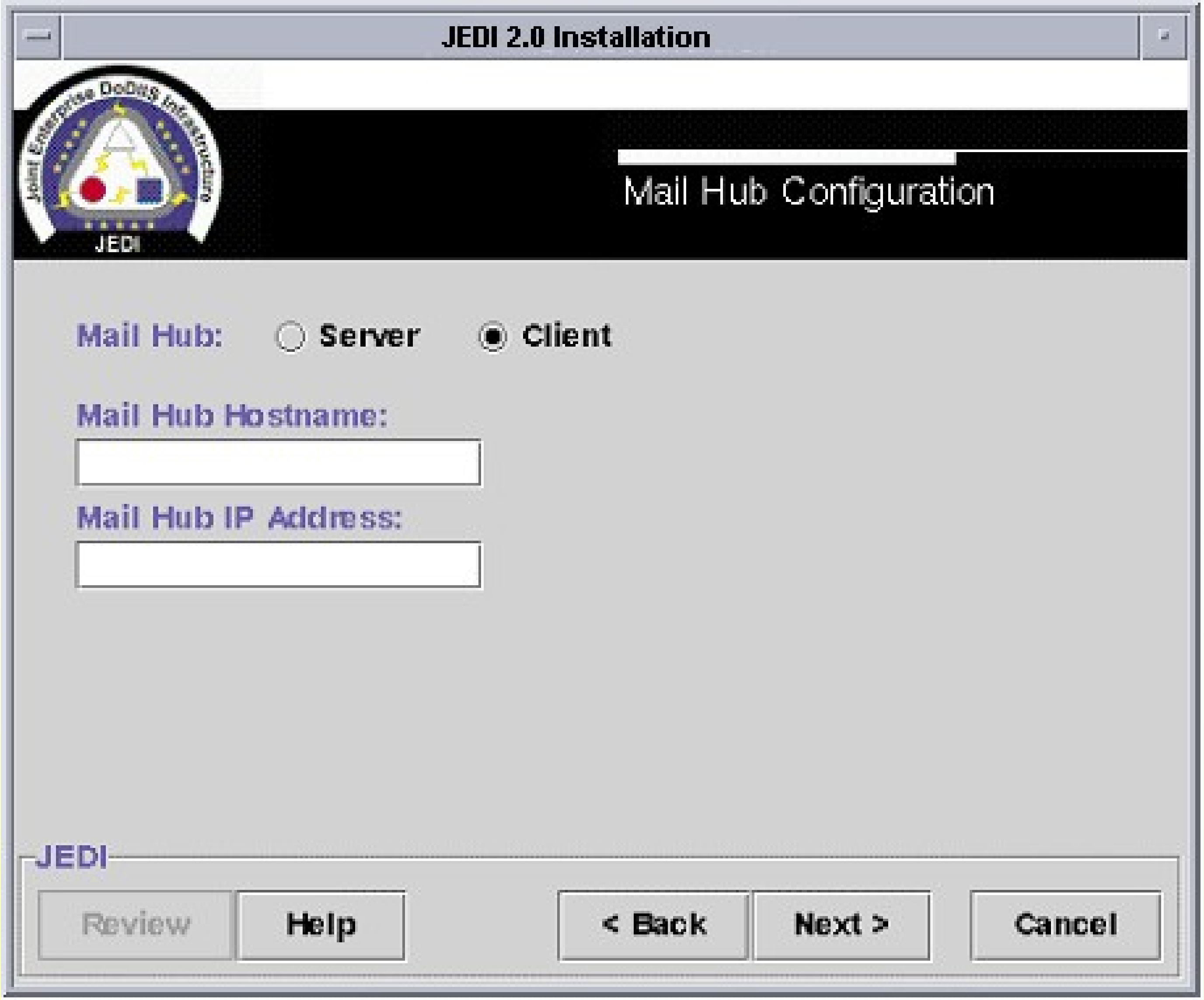
Mail Hub Configuration

Mail Hub: ● Server ○ Client

Mail Hub Clients:

Enter the name of mail clients to this host (One per line)

Solaris 9 – JEDI PreInstallation



JEDI 2.0 Installation

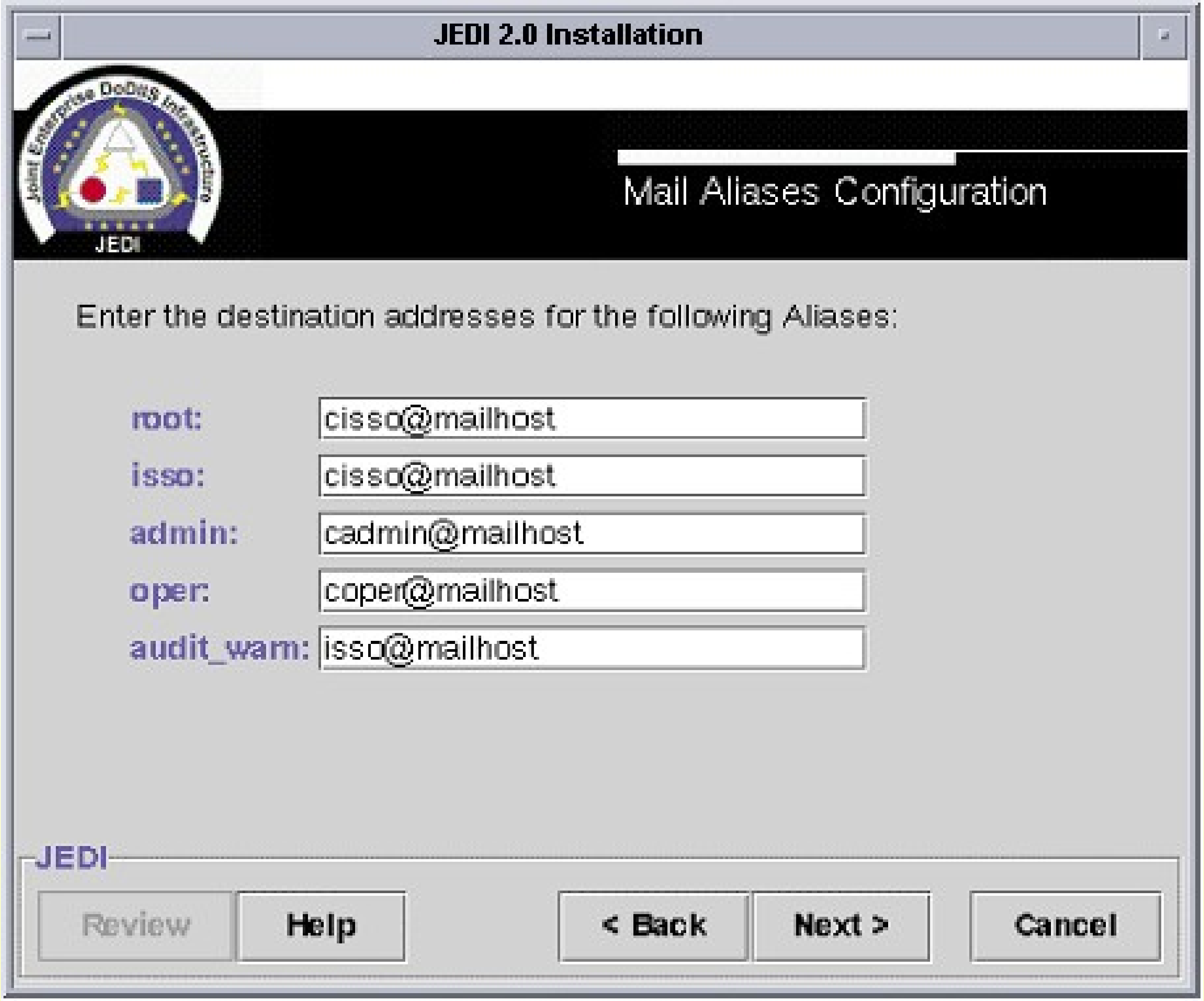
Mail Hub Configuration

Mail Hub: ○ Server ● Client

Mail Hub Hostname:

Mail Hub IP Address:

Solaris 9 – JEDI PreInstallation



Mail Aliases Configuration

Enter the destination addresses for the following Aliases:

root: cisso@mailhost

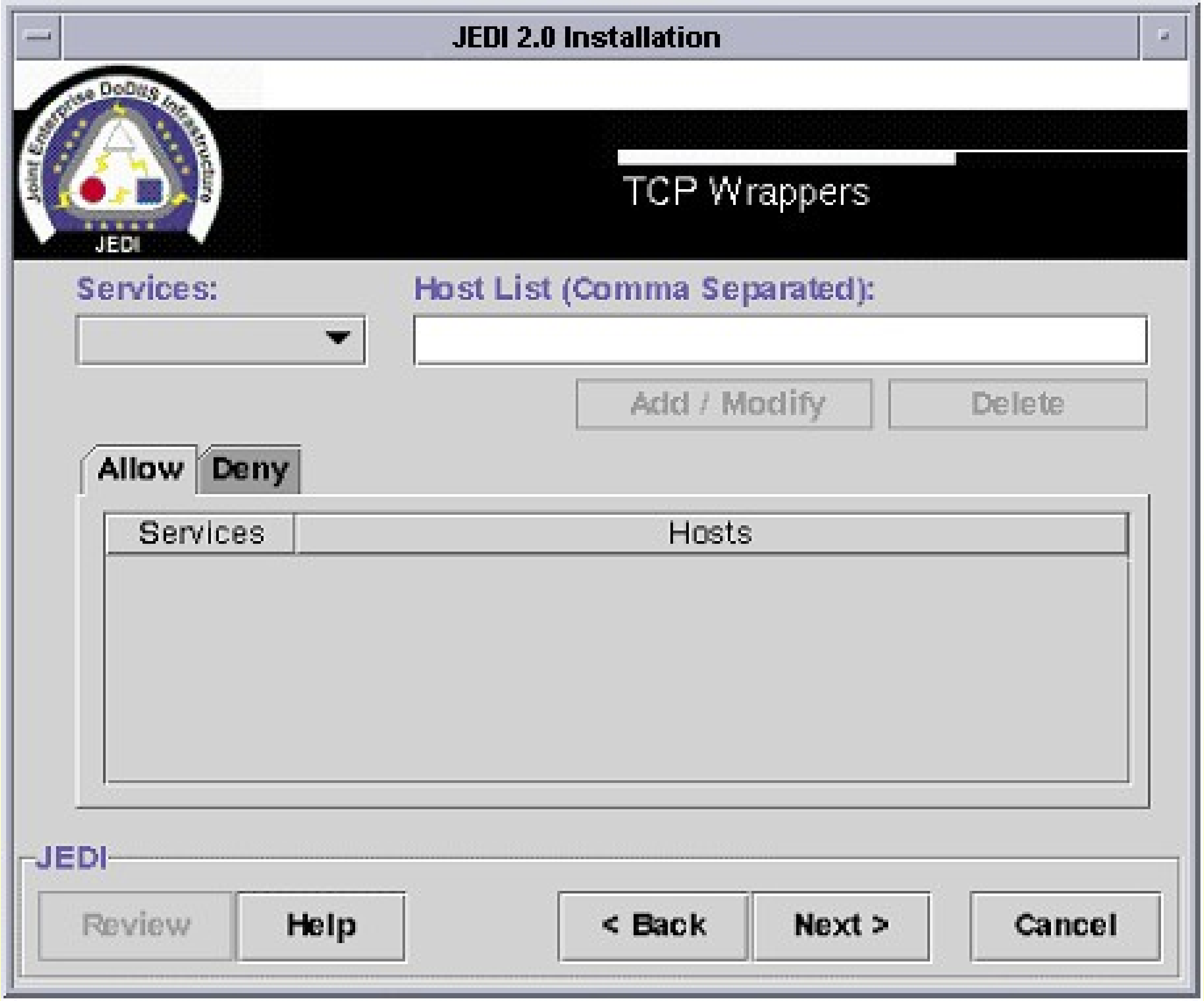
isso: cisso@mailhost

admin: cadmin@mailhost

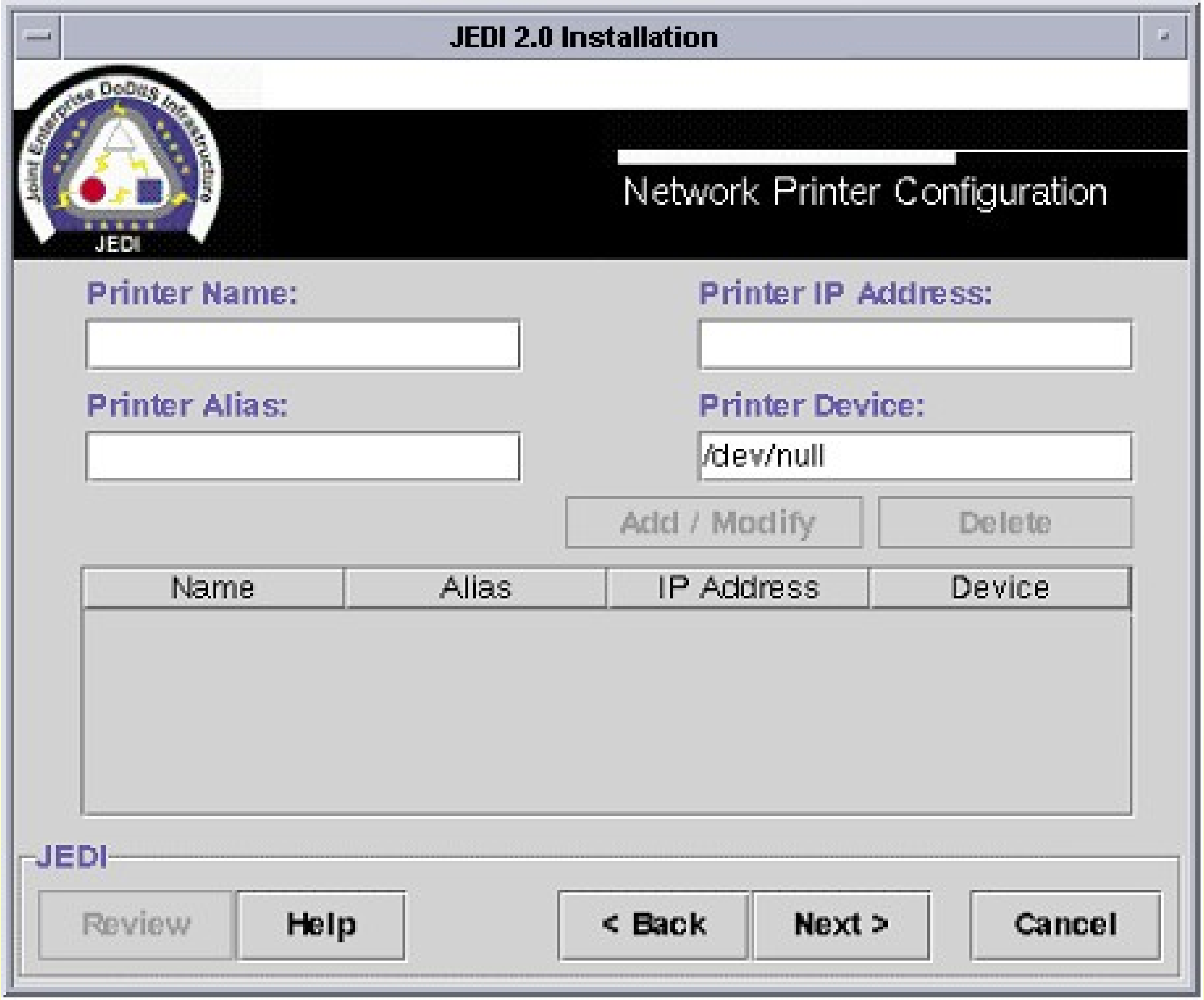
oper: coper@mailhost

audit_warn: isso@mailhost

Solaris 9 – JEDI PreInstallation



Solaris 9 – JEDI PreInstallation



JEDI 2.0 Installation

Network Printer Configuration

Printer Name:

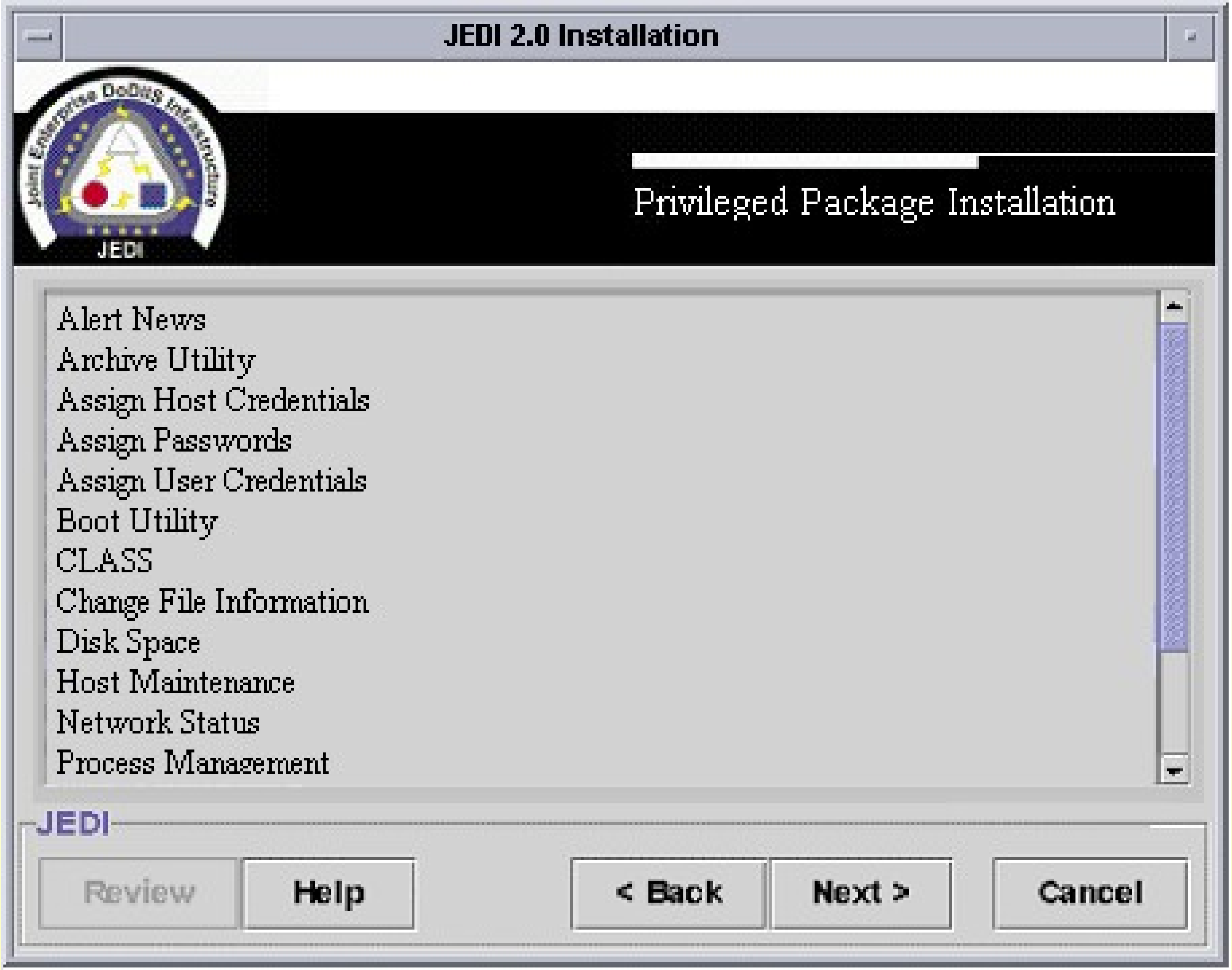
Printer IP Address:

Printer Alias:

Printer Device: /dev/null

Name	Alias	IP Address	Device

Solaris 9 – JEDI PreInstallation

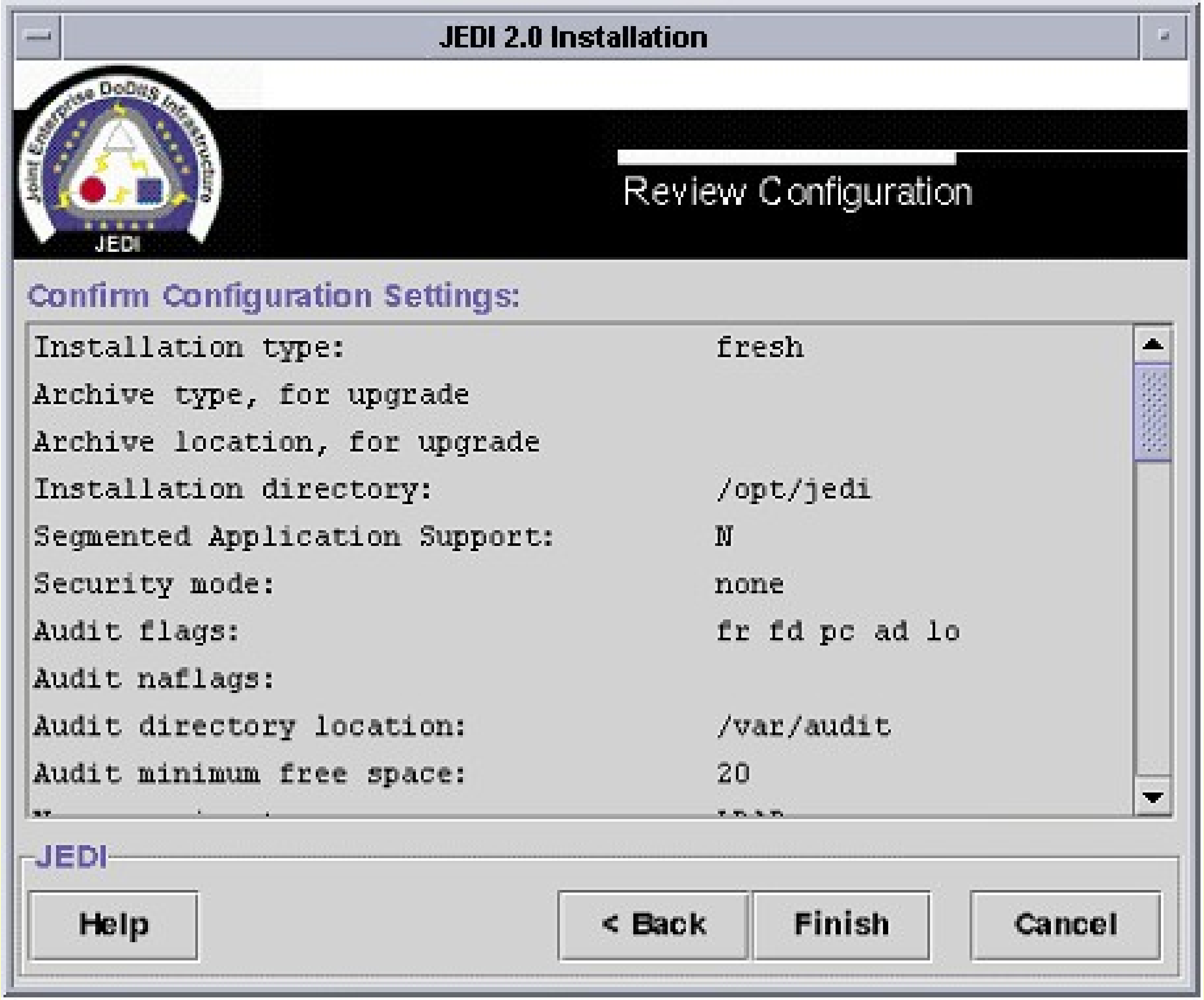


JEDI 2.0 Installation

Privileged Package Installation

Alert News
Archive Utility
Assign Host Credentials
Assign Passwords
Assign User Credentials
Boot Utility
CLASS
Change File Information
Disk Space
Host Maintenance
Network Status
Process Management

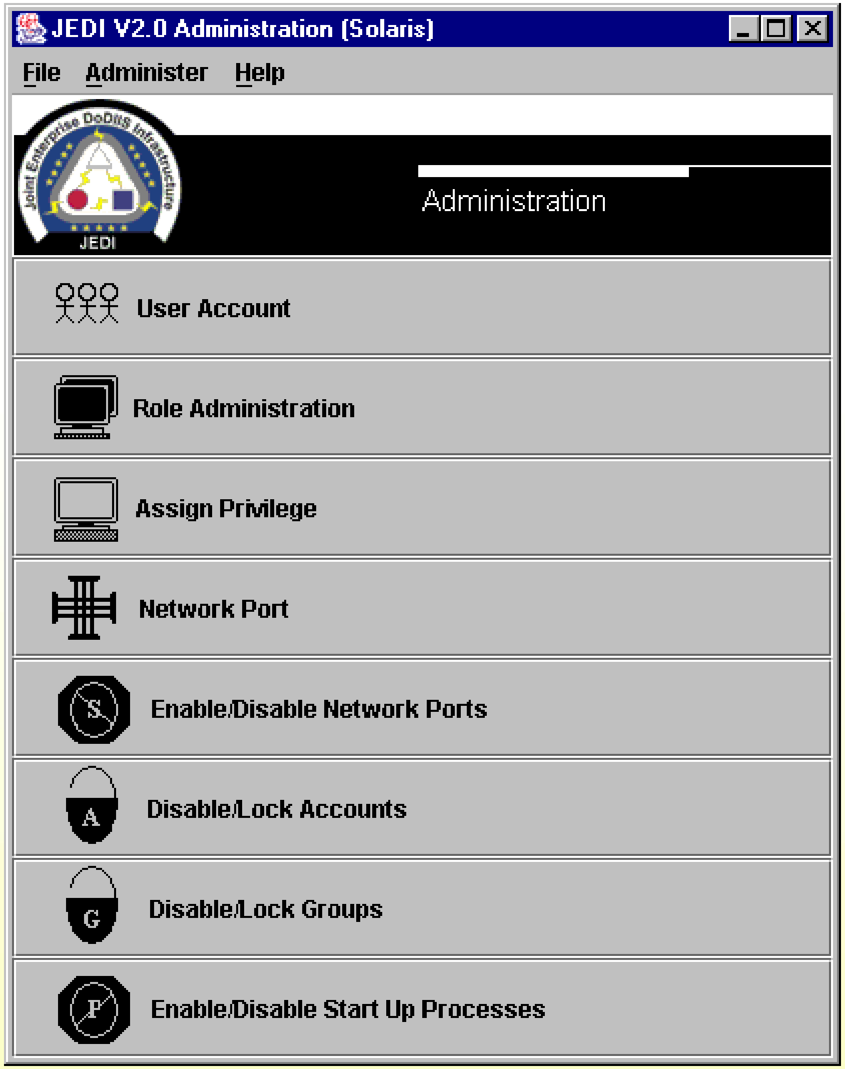
Solaris 9 – JEDI PreInstallation



Confirm Configuration Settings:

```
Installation type:                       fresh
Archive type, for upgrade
Archive location, for upgrade
Installation directory:                  /opt/jedi
Segmented Application Support:           N
Security mode:                           none
Audit flags:                             fr fd pc ad lo
Audit naflags:
Audit directory location:                /var/audit
Audit minimum free space:                20
```

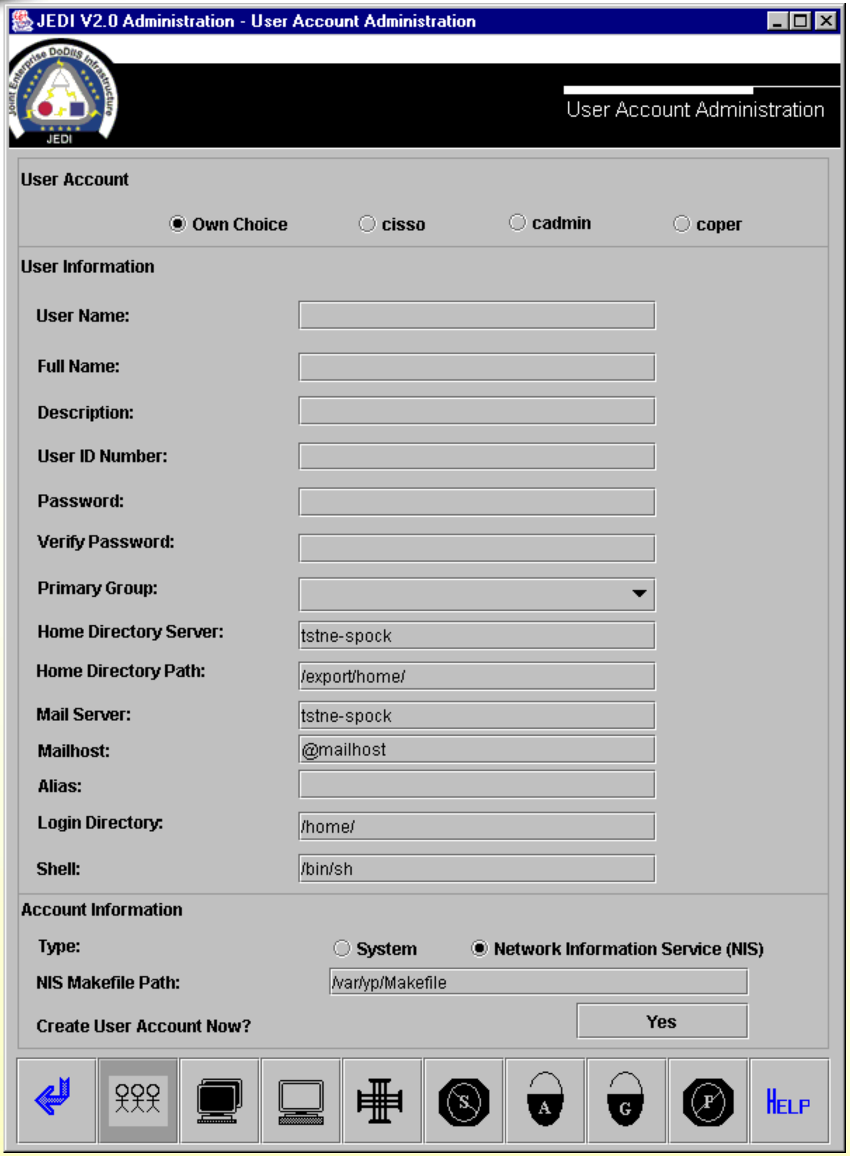
Solaris 9 – JEDI PostInstallation



- Administration, Setup, and DNS installation GUIs will be reengineered in Java
- Underlying support scripts will support Jumpstart Installations

NORTHROP GRUMMAN
Information Technology

Solaris 9 – JEDI PostInstallation



JEDI V2.0 Administration - User Account Administration

User Account Administration

User Account

● Own Choice ○ cisso ○ cadmin ○ coper

User Information

User Name:	
Full Name:	
Description:	
User ID Number:	
Password:	
Verify Password:	
Primary Group:	
Home Directory Server:	tstne-spock
Home Directory Path:	/export/home/
Mail Server:	tstne-spock
Mailhost:	@mailhost
Alias:	
Login Directory:	/home/
Shell:	/bin/sh

Account Information

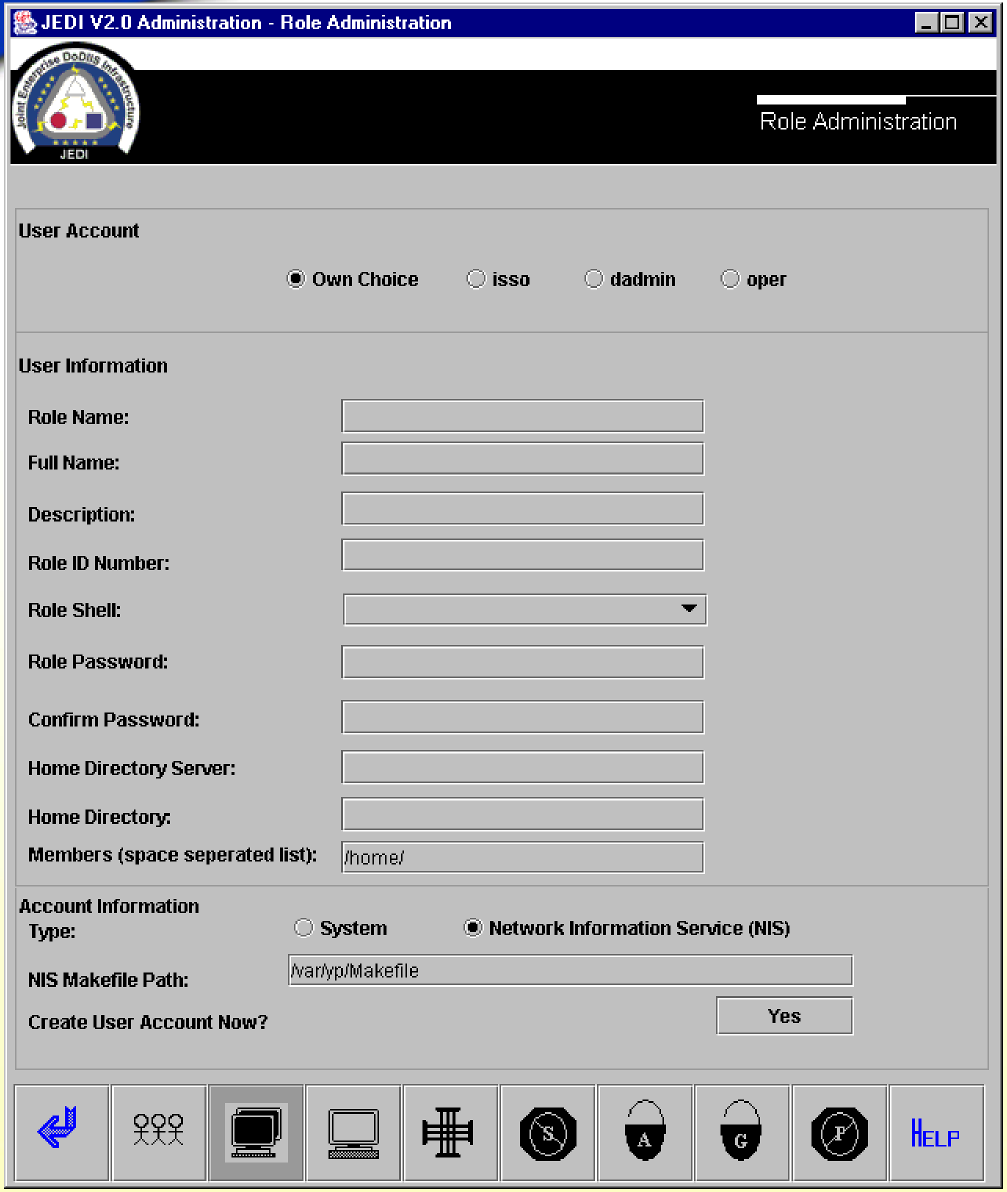
Type: ○ System ● Network Information Service (NIS)

NIS Makefile Path: /var/yp/Makefile

Create User Account Now? Yes

- **User Account Administration**
  - Creates user accounts on the system
    - Fields mirror data collected for SMC
      - Add User Wizard
    - Default fields will be set for SMC including Primary Project

Solaris 9 – JEDI PostInstallation



JEDI V2.0 Administration - Role Administration

Role Administration

User Account

● Own Choice ○ isso ○ dadmin ○ oper

User Information

Role Name:	
Full Name:	
Description:	
Role ID Number:	
Role Shell:	
Role Password:	
Confirm Password:	
Home Directory Server:	
Home Directory:	
Members (space seperated list):	/home/

Account Information

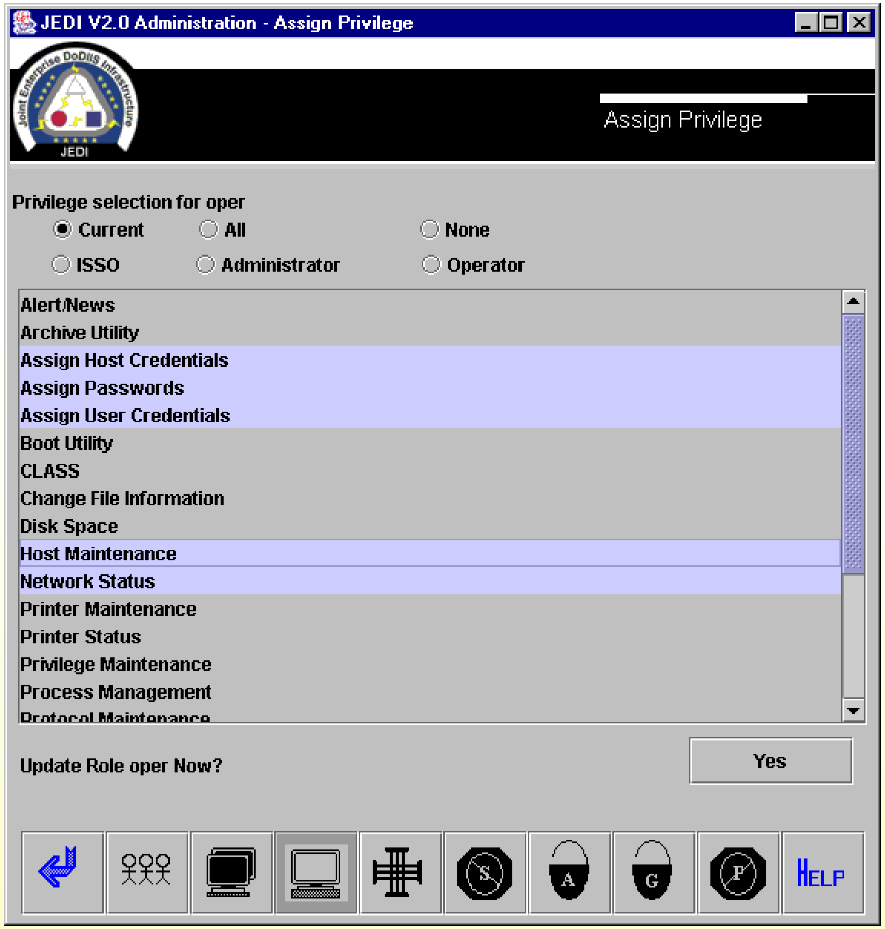
Type: ○ System ● Network Information Service (NIS)

NIS Makefile Path: /var/yp/Makefile

Create User Account Now? Yes

- **Role Administration**
  - Creates roles on the system
    - Fields mirror data collected for SMC
      - Role Creation Wizard
    - Default fields will be set for SMC including Primary Project

Solaris 9 – JEDI PostInstallation



JEDI V2.0 Administration - Assign Privilege

Assign Privilege

Privilege selection for oper

● Current ○ All ○ None

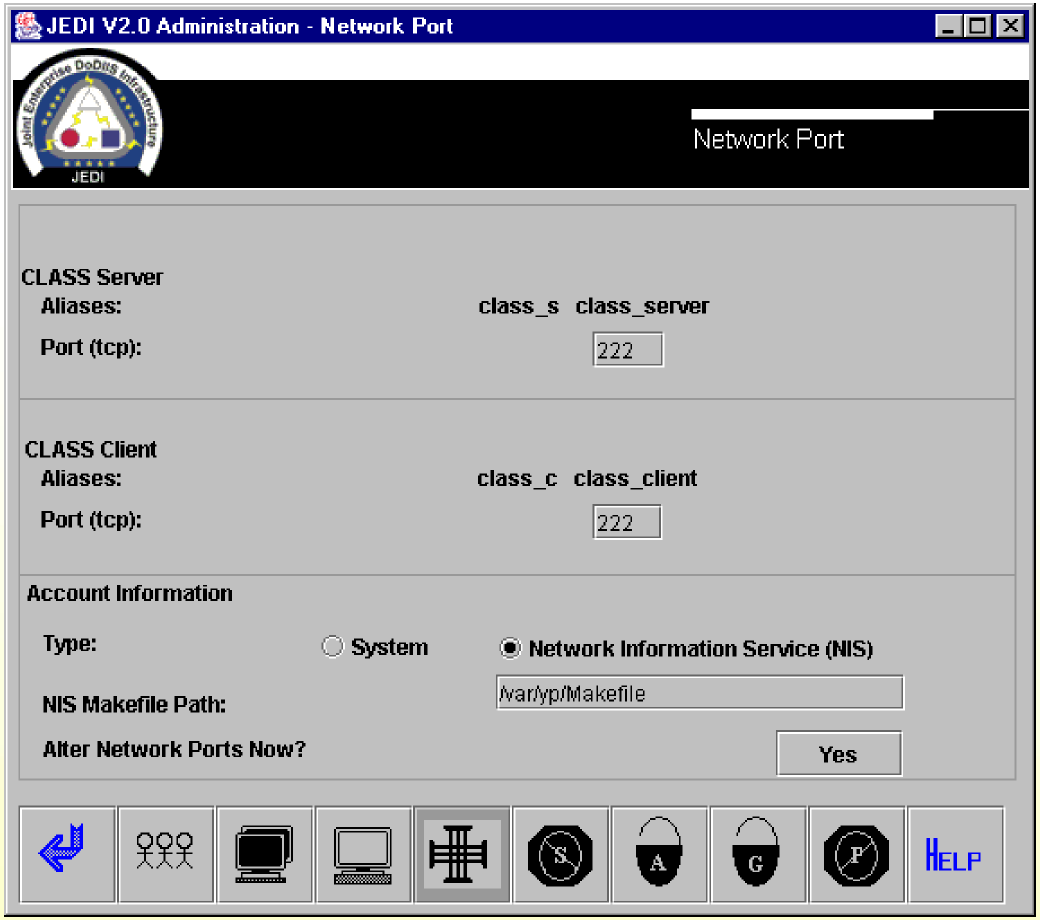
○ ISSO ○ Administrator ○ Operator

Alert/News
Archive Utility
Assign Host Credentials
Assign Passwords
Assign User Credentials
Boot Utility
CLASS
Change File Information
Disk Space
Host Maintenance
Network Status
Printer Maintenance
Printer Status
Privilege Maintenance
Process Management
Protocol Maintenance

Update Role oper Now?

- **Assign Privilege**
  - Assign Rights to chosen roles
    - Reads /etc/security/prof_attr
    - Updates /etc/user_attr

Solaris 9 – JEDI PostInstallation



JEDI V2.0 Administration - Network Port

Network Port

CLASS Server

Aliases: class_s class_server

Port (tcp): 222

CLASS Client

Aliases: class_c class_client

Port (tcp): 222

Account Information

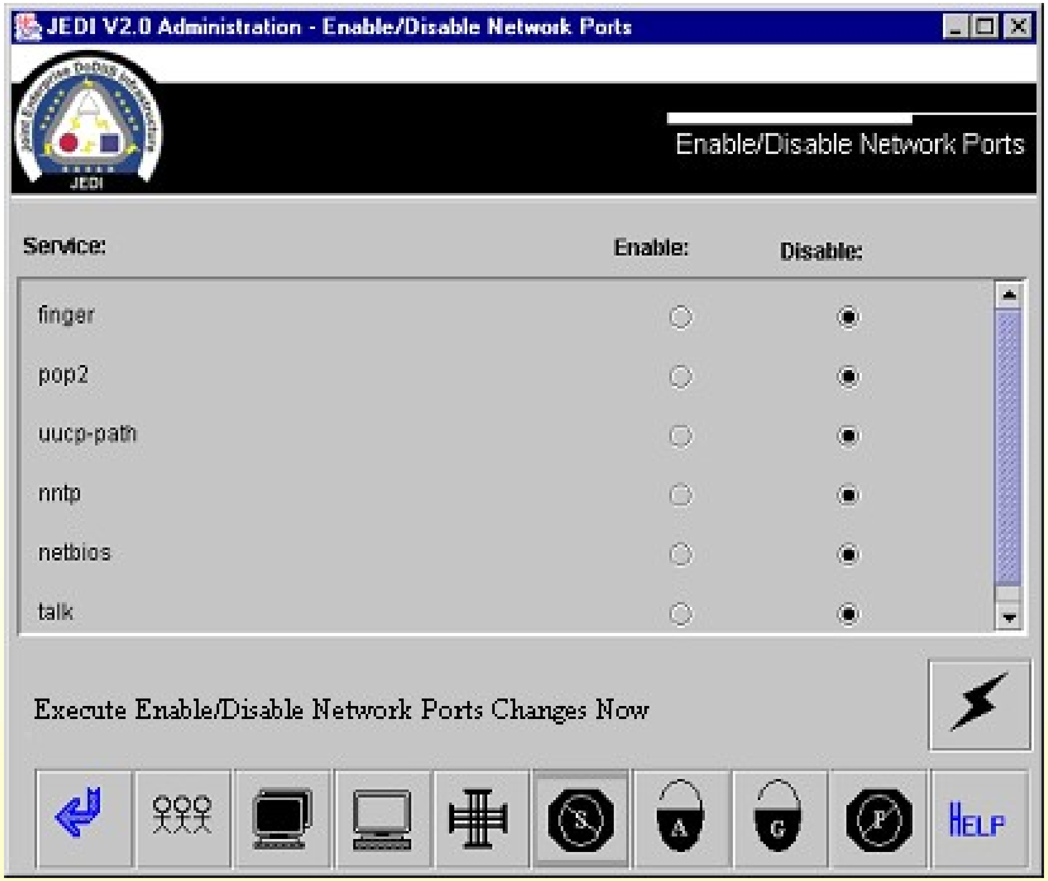
Type: ○ System ● Network Information Service (NIS)

NIS Makefile Path: /var/yp/Makefile

Alter Network Ports Now? Yes

- **Network Port**
  - Sets port for CLASS
  - Sets Makefile path

Solaris 9 – JEDI PostInstallation



JEDI V2.0 Administration - Enable/Disable Network Ports

Enable/Disable Network Ports

Service:	Enable:	Disable:
finger	○	●
pop2	○	●
uucp-path	○	●
nntp	○	●
netbios	○	●
talk	○	●

Execute Enable/Disable Network Ports Changes Now

- **Enable/Disable Network Ports**
  - Displays contents of services file
  - Services recommended for disabling are displayed at the top of the scrollable list
  - Updates the JASS_SVCS_DISABLE variable in the JASS configuration file
    - On subsequent runs of JASS, the specified services will be disabled

NORTHROP GRUMMAN
Information Technology

Solaris 9 – JEDI PostInstallation

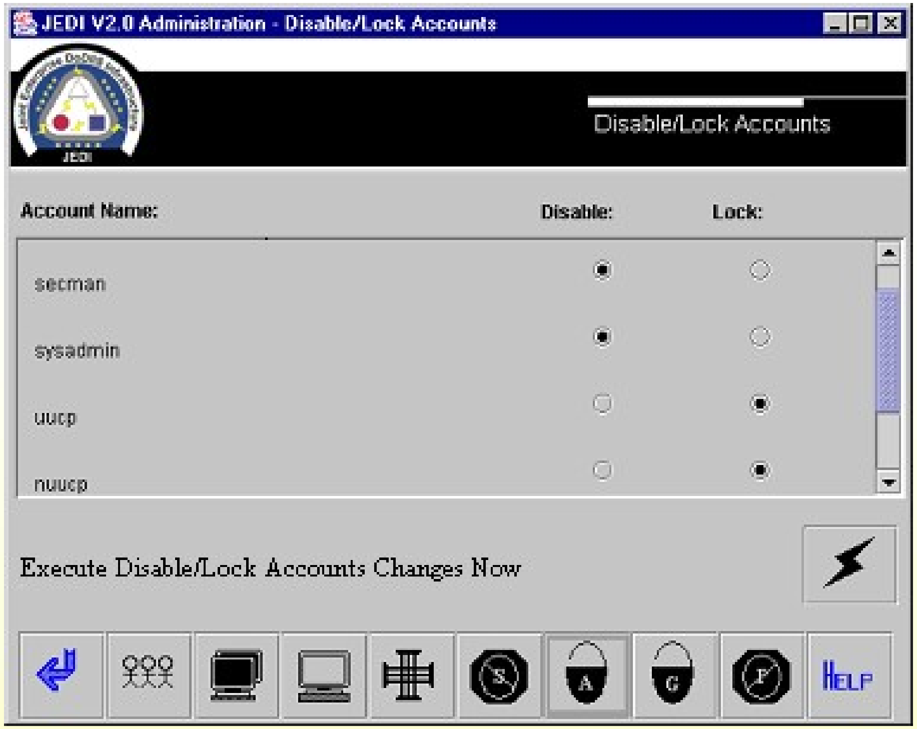
- **Recommended Services to disable**

Kshell
New-rwho
Rmonitor
Monitor
Pcserver
Sun-dr
Kerberos
Krb5-pop
Cvc
www-ldap
Klogin
Snmp (client)
Echo
uucp

Discard
sysstat
daytime
chargen
time
name
whois
bootps
bootpc
hostnames
pop2
pop3
Imap
Biff
rping

submissiona
rje
finger
x400
X400-smb
Csnet-ns
Uucp-path
nntp
netbios
slp
Mobile-ip
Cvc-hostid
Courier
talk

Solaris 9 – JEDI PostInstallation



JEDI V2.0 Administration - Disable/Lock Accounts

Disable/Lock Accounts

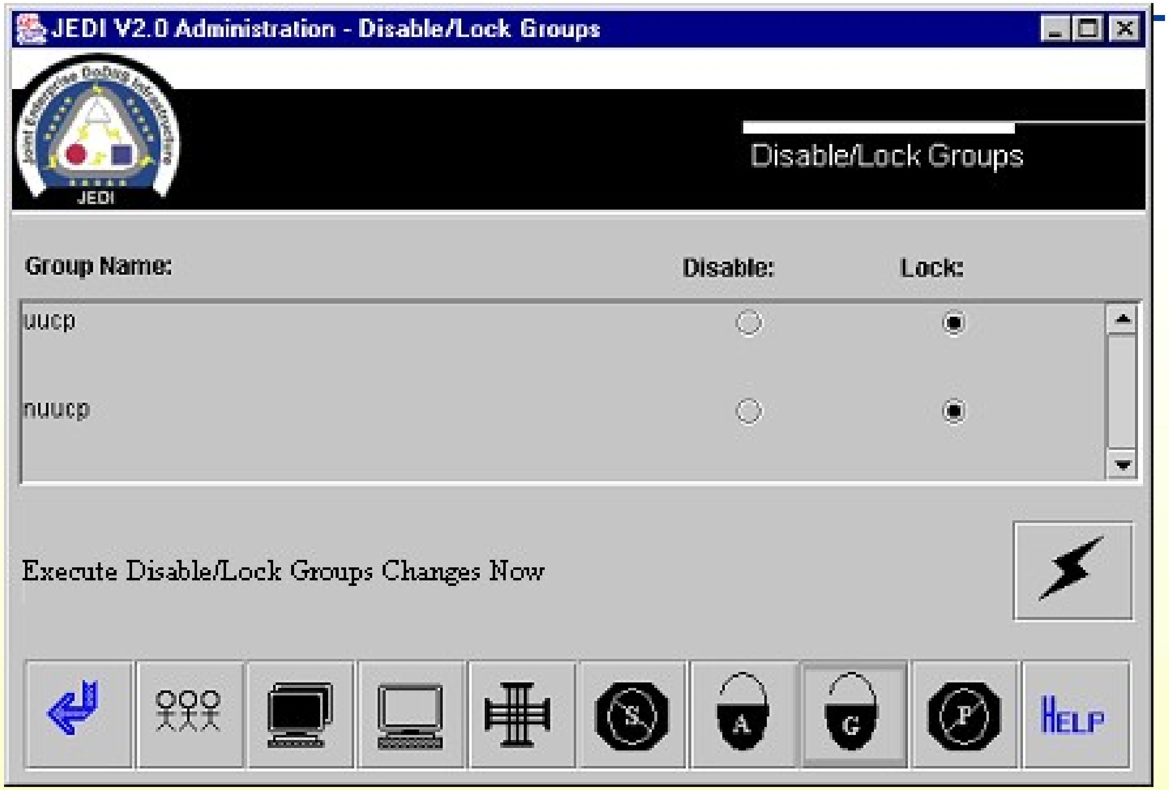
Account Name:	Disable:	Lock:
secman	●	○
sysadmin	●	○
uucp	○	●
nuucp	○	●

Execute Disable/Lock Accounts Changes Now

- **Disable/Lock Accounts**
  - Displays contents of passwd file
  - Accounts recommended for locking or disabling are displayed at the top of the scrollable list
  - Updates the JASS_ACCT_DISABLE and JASS_ACCT_REMOVE variables in the JASS configuration file
    - On subsequent runs of JASS, the specified users will be disabled

Solaris 9 – JEDI PostInstallation

- **Disable/Lock Groups**
  - Reads the contents of the group file
    - Groups recommended for disable/lock are displayed at the top



JEDI V2.0 Administration - Disable/Lock Groups

Disable/Lock Groups

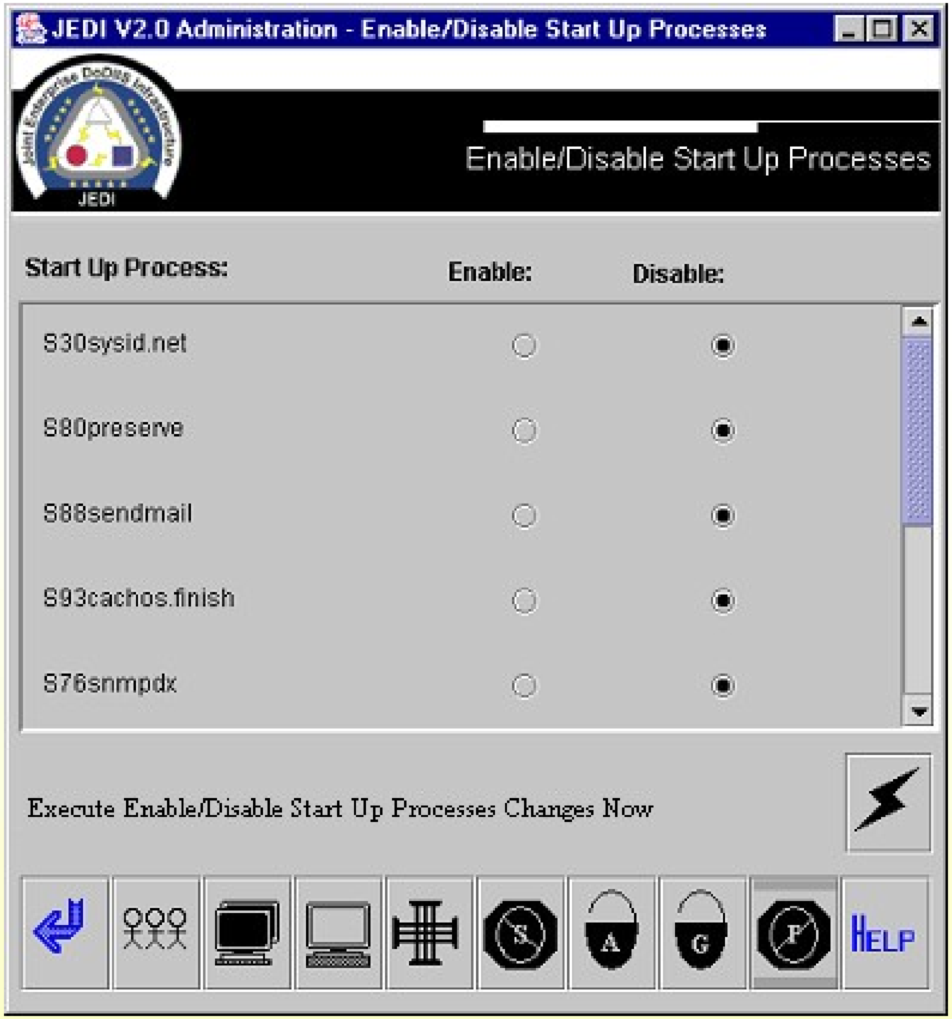
Group Name:	Disable:	Lock:
uucp	○	●
nuucp	○	●

Execute Disable/Lock Groups Changes Now

Solaris 9 – JEDI PostInstallation

- **Accounts recommended for disabling**
  - SA
  - COE
  - Keyman
  - SSO
  - Secman
  - Sysadmin
- **Accounts recommended for locking**
  - Uucp
  - Nuucp
  - Nobody
  - Listen
- **Groups recommended for locking**
  - Uucp
  - Nuucp

Solaris 9 – JEDI PostInstallation



JEDI V2.0 Administration - Enable/Disable Start Up Processes

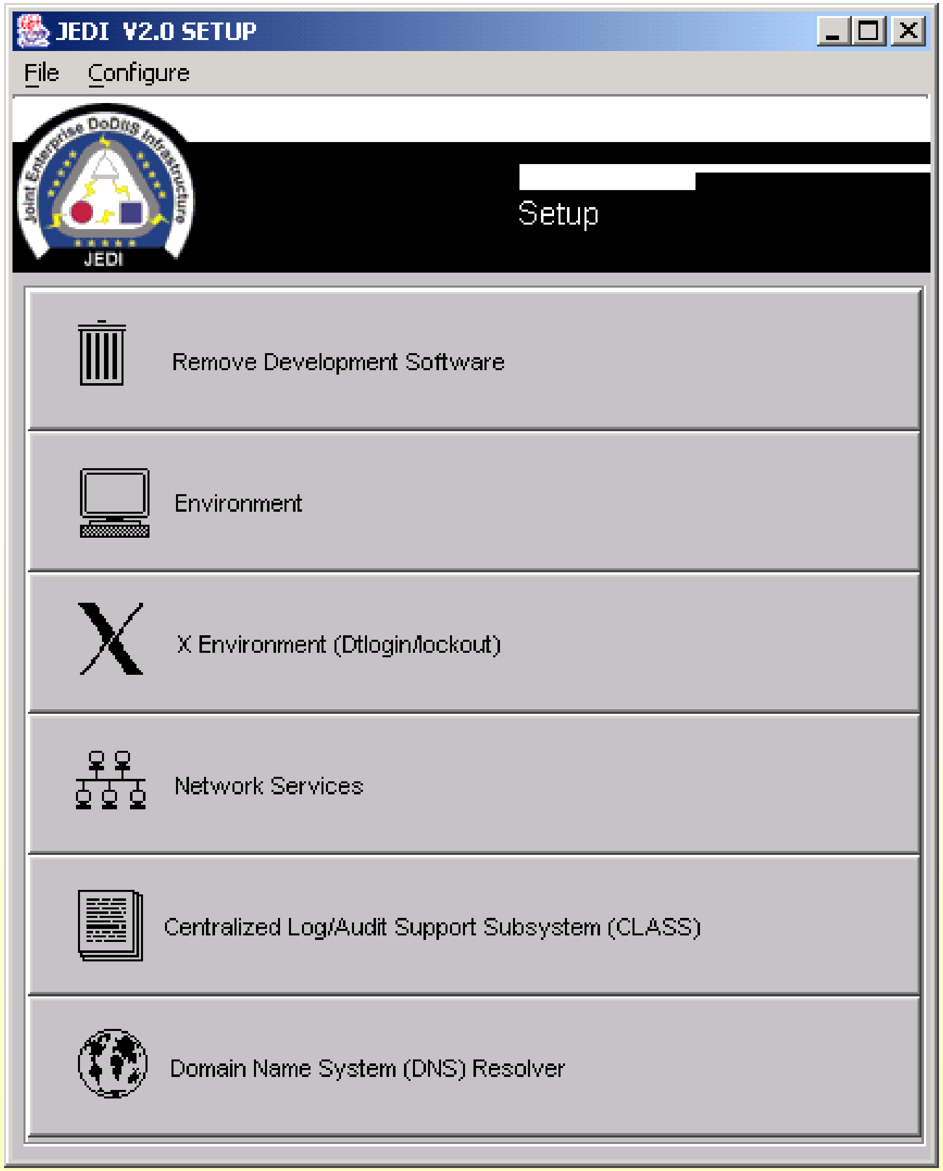
Enable/Disable Start Up Processes

Start Up Process:	Enable:	Disable:
S30sysid.net	○	●
S80preserve	○	●
S88sendmail	○	●
S93cachos.finish	○	●
S76snmpdx	○	●

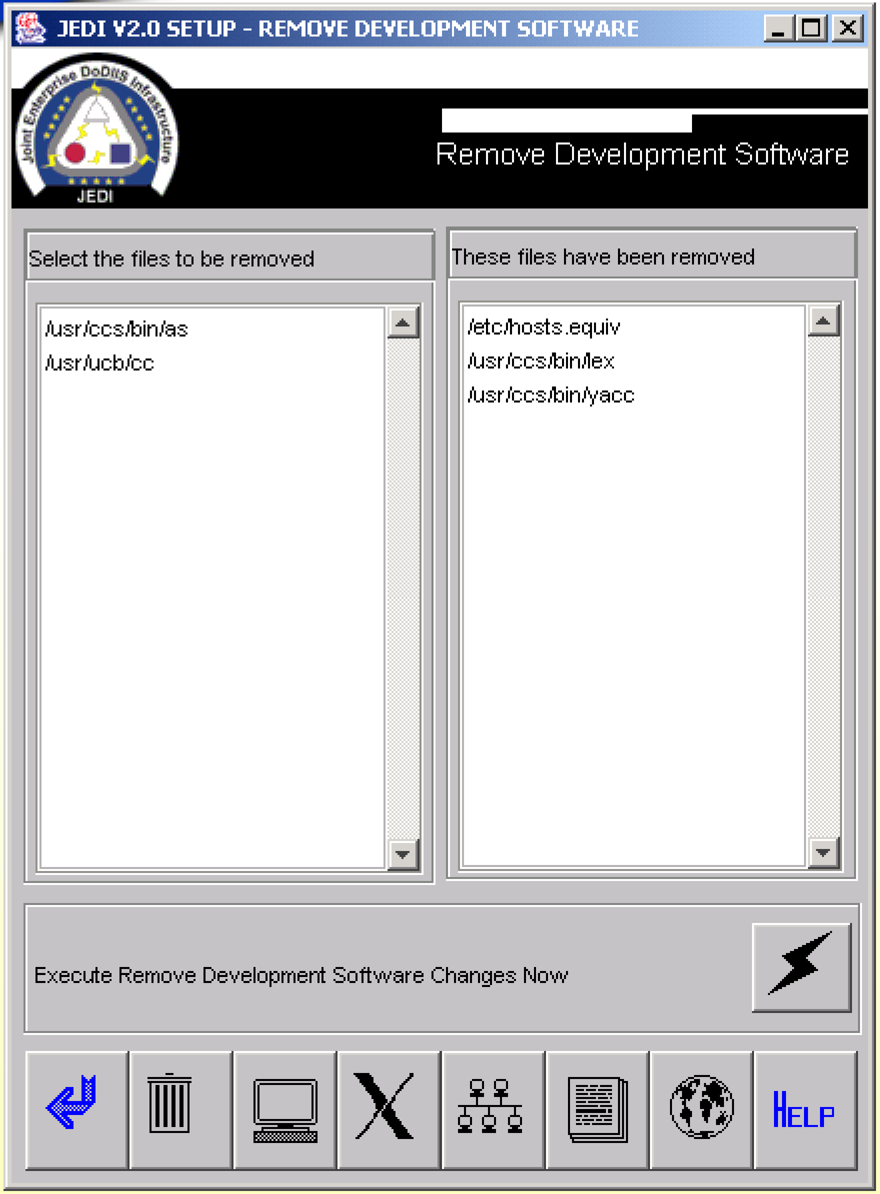
Execute Enable/Disable Start Up Processes Changes Now

- **Enable/Disable Start Up Processes**
  - Displays a list of processes recommended for disabling
  - Sets the uppercase first letter in the startup script name to lower case
    - Script will not be executed

Solaris 9 – JEDI PostInstallation


JEDI V2.0 SETUP
File
Configure
Joint Enterprise DoDIIS Infrastructure
JEDI
Setup
Remove Development Software
Environment
X Environment (Dtlogin/lockout)
Network Services
Centralized Log/Audit Support Subsystem (CLASS)
Domain Name System (DNS) Resolver

Solaris 9 – JEDI PostInstallation


JEDI V2.0 SETUP - REMOVE DEVELOPMENT SOFTWARE
Joint Enterprise DoDIIS Infrastructure
JEDI
Remove Development Software
Execute Remove Development Software Changes Now
HELP

Select the files to be removed

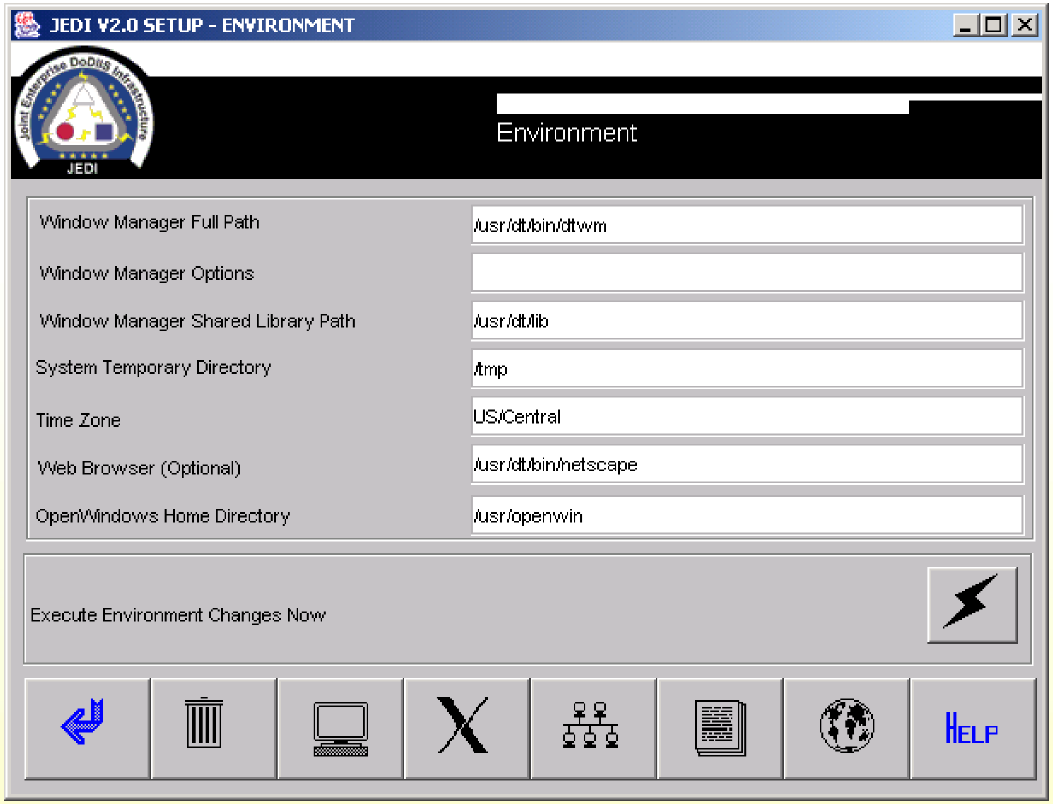
```
/usr/ccs/bin/as
/usr/ucb/cc
```

These files have been removed

```
/etc/hosts.equiv
/usr/ccs/bin/lex
/usr/ccs/bin/yacc
```

- **Remove Development Software**
  - Removes development packages from the system

Solaris 9 – JEDI PostInstallation



JEDI V2.0 SETUP - ENVIRONMENT

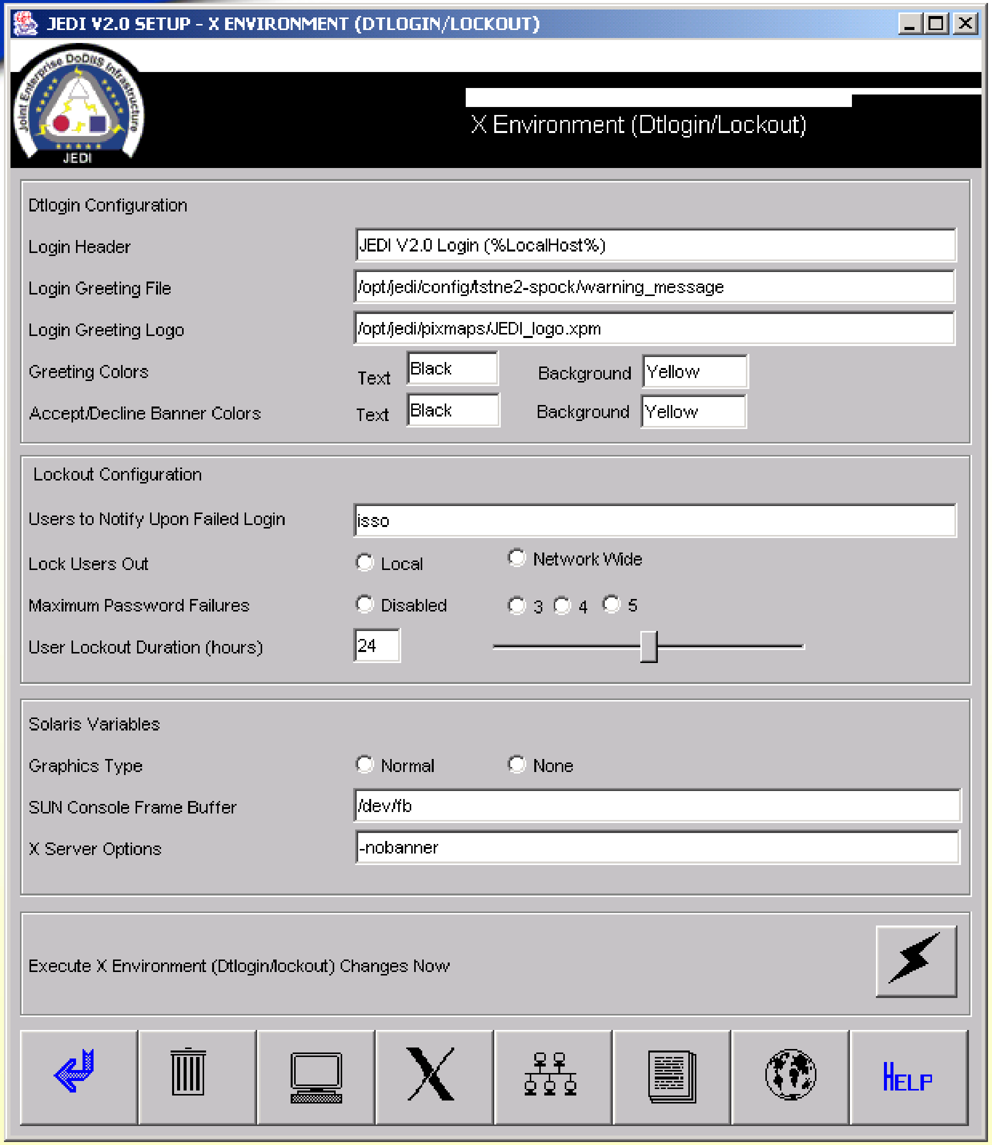
Environment

Window Manager Full Path	/usr/dt/bin/dtwm
Window Manager Options	
Window Manager Shared Library Path	/usr/dt/lib
System Temporary Directory	/tmp
Time Zone	US/Central
Web Browser (Optional)	/usr/dt/bin/netscape
OpenWindows Home Directory	/usr/openwin

Execute Environment Changes Now

- **Environment**
  - Environment Settings for
    - Window Manager
    - Temp directory
    - Time Zone
    - Web Browser
    - Open Windows Home Directory

Solaris 9 – JEDI PostInstallation



JEDI V2.0 SETUP - X ENVIRONMENT (DTLOGIN/LOCKOUT)

X Environment (Dtlogin/Lockout)

Dtlogin Configuration

Login Header: JEDI V2.0 Login (%LocalHost%)

Login Greeting File: /opt/jedi/config/tstne2-spock/warning_message

Login Greeting Logo: /opt/jedi/pixmaps/JEDI_logo.xpm

Greeting Colors: Text Black Background Yellow

Accept/Decline Banner Colors: Text Black Background Yellow

Lockout Configuration

Users to Notify Upon Failed Login: isso

Lock Users Out: ○ Local ○ Network Wide

Maximum Password Failures: ○ Disabled ○ 3 ○ 4 ○ 5

User Lockout Duration (hours): 24

Solaris Variables

Graphics Type: ○ Normal ○ None

SUN Console Frame Buffer: /dev/fb

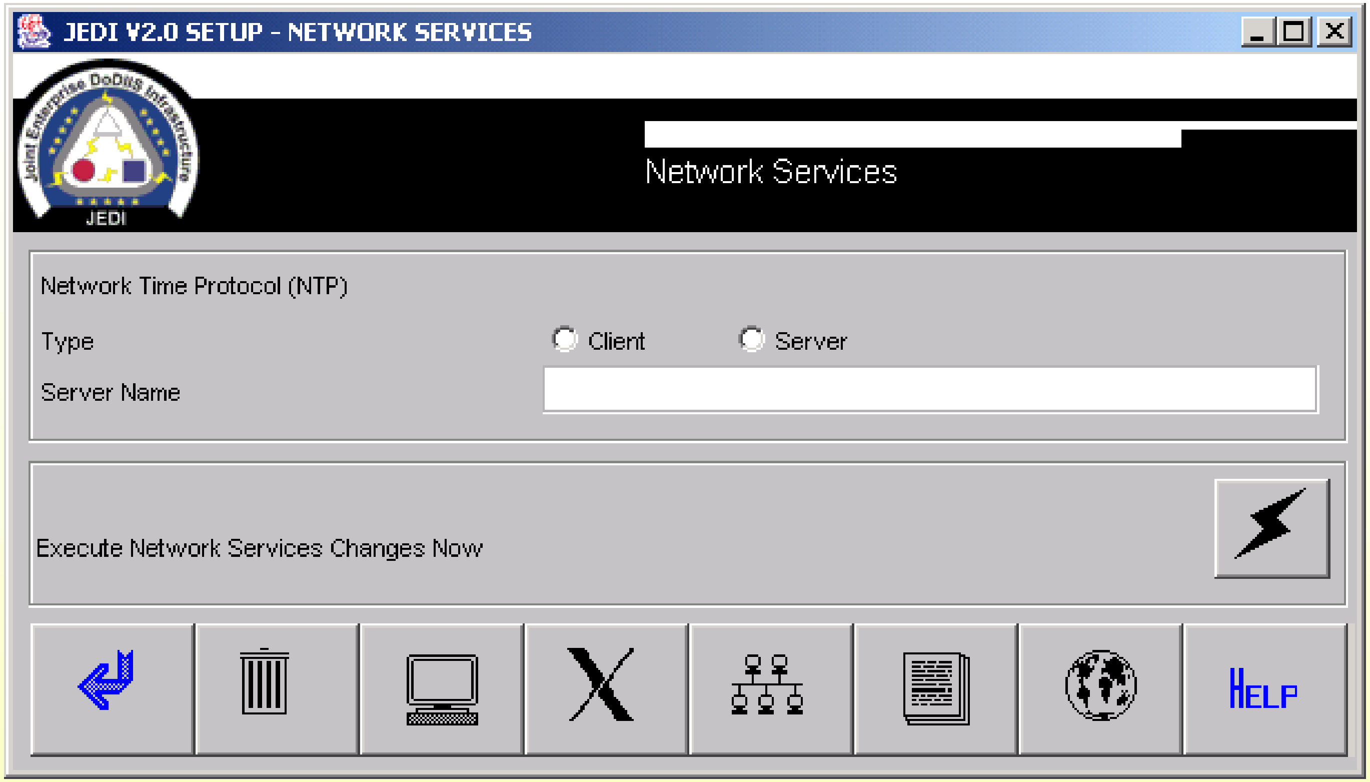
X Server Options: -nobanner

Execute X Environment (Dtlogin/lockout) Changes Now

- **X Environment**
  - Environment Settings for
    - Login Header
    - Login Greeting
    - Colors
    - Lockout Configuration
    - Frame Buffer
    - X Server Options

Solaris 9 – JEDI PostInstallation

- **Network Services**
  - Network Time Protocol Settings



JEDI V2.0 SETUP - NETWORK SERVICES

Network Services

Network Time Protocol (NTP)

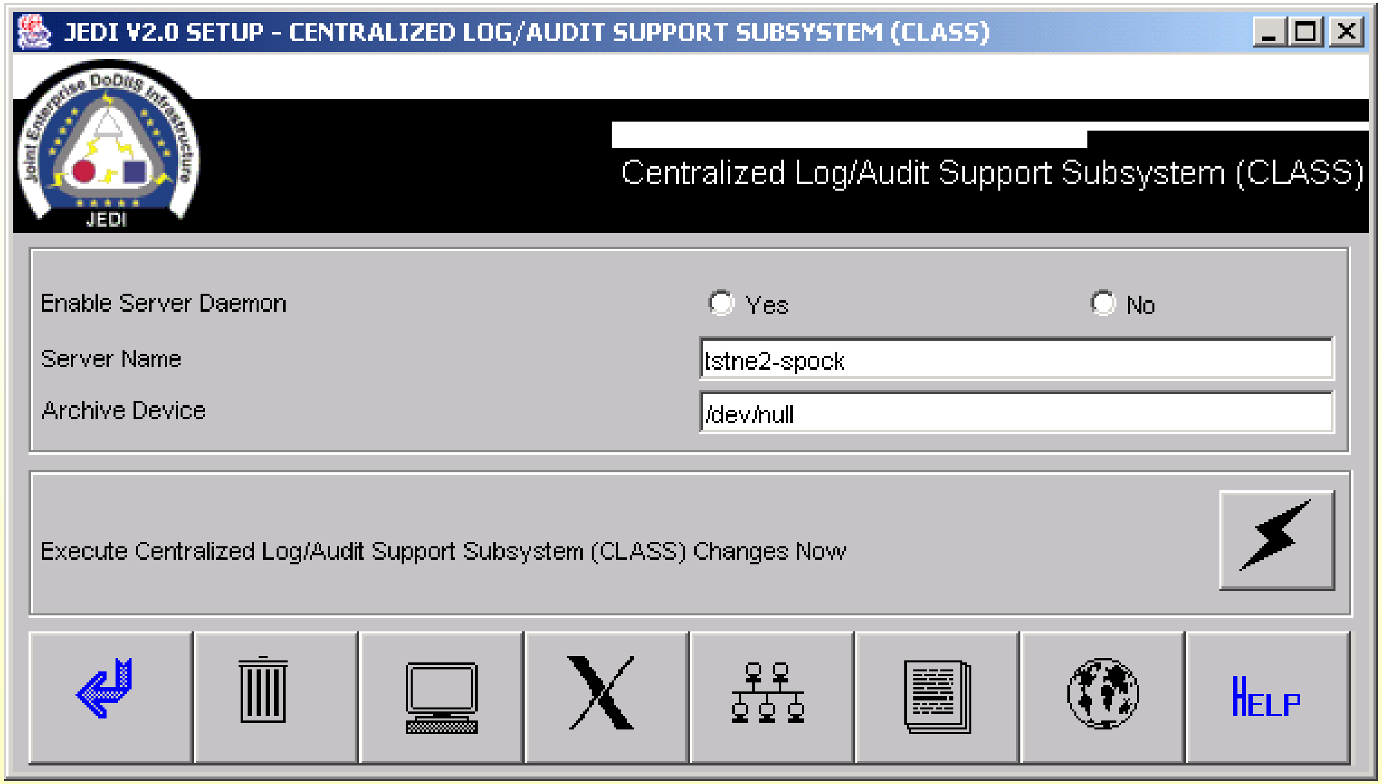
Type ○ Client ○ Server

Server Name

Execute Network Services Changes Now

Solaris 9 – JEDI PostInstallation

- **CLASS**
  - Settings for CLASS client and server



JEDI V2.0 SETUP - CENTRALIZED LOG/AUDIT SUPPORT SUBSYSTEM (CLASS)

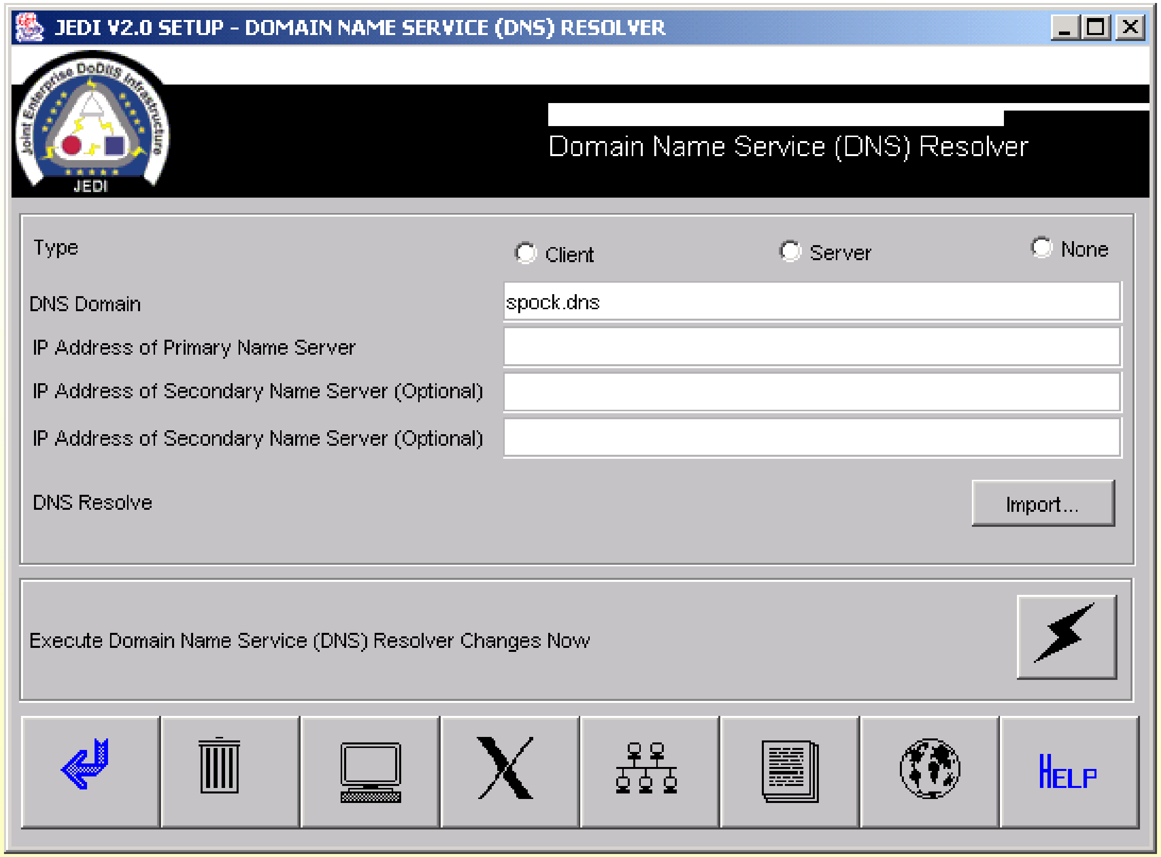
Centralized Log/Audit Support Subsystem (CLASS)

Enable Server Daemon	○ Yes	○ No
Server Name	tstne2-spock	
Archive Device	/dev/null	

Execute Centralized Log/Audit Support Subsystem (CLASS) Changes Now

Solaris 9 – JEDI PostInstallation

- **DNS Resolver**
  - Configures workstation as a DNS client



JEDI V2.0 SETUP - DOMAIN NAME SERVICE (DNS) RESOLVER

Domain Name Service (DNS) Resolver

Type ○ Client ○ Server ○ None

DNS Domain: spock.dns

IP Address of Primary Name Server:

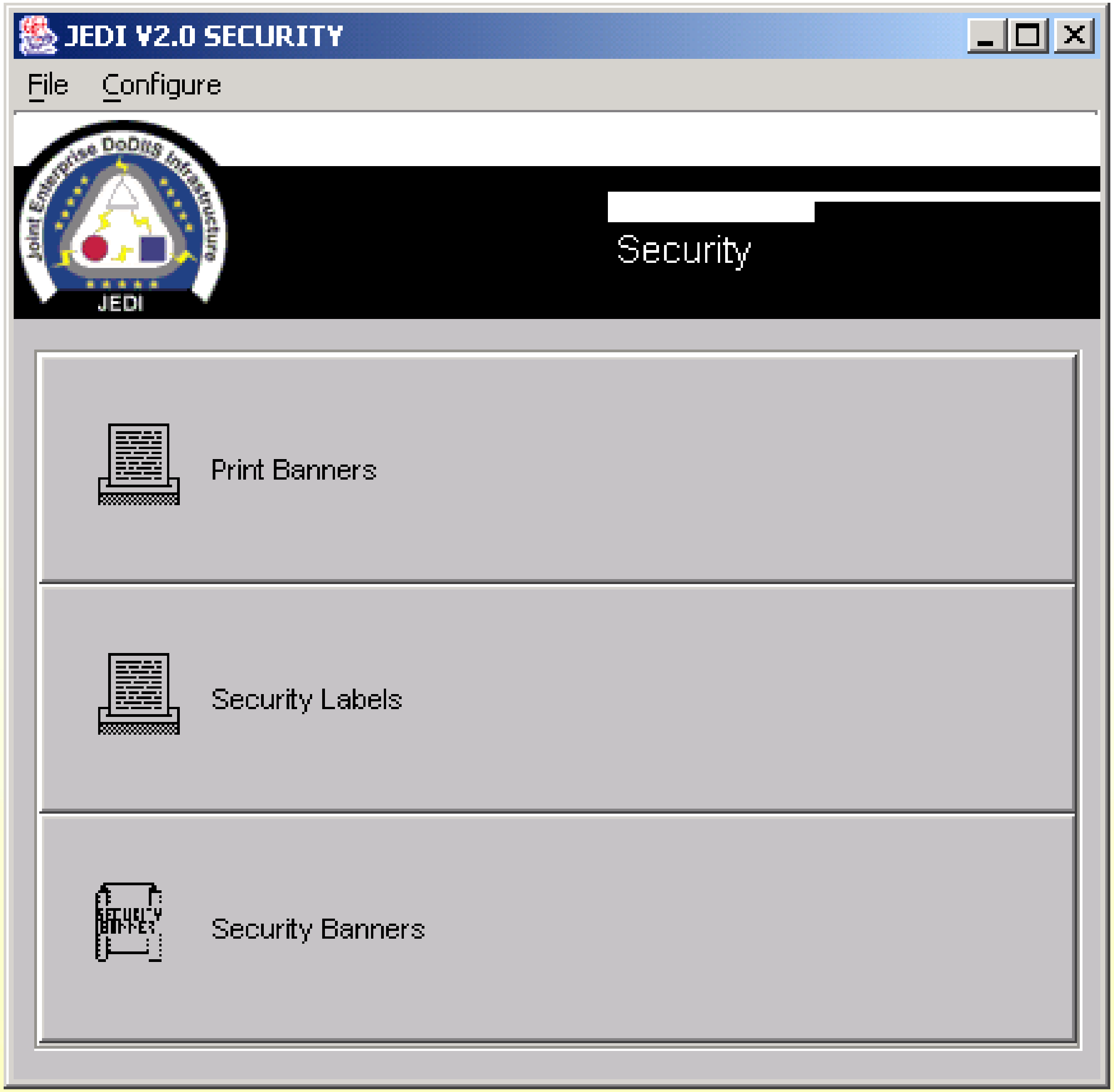
IP Address of Secondary Name Server (Optional):

IP Address of Secondary Name Server (Optional):

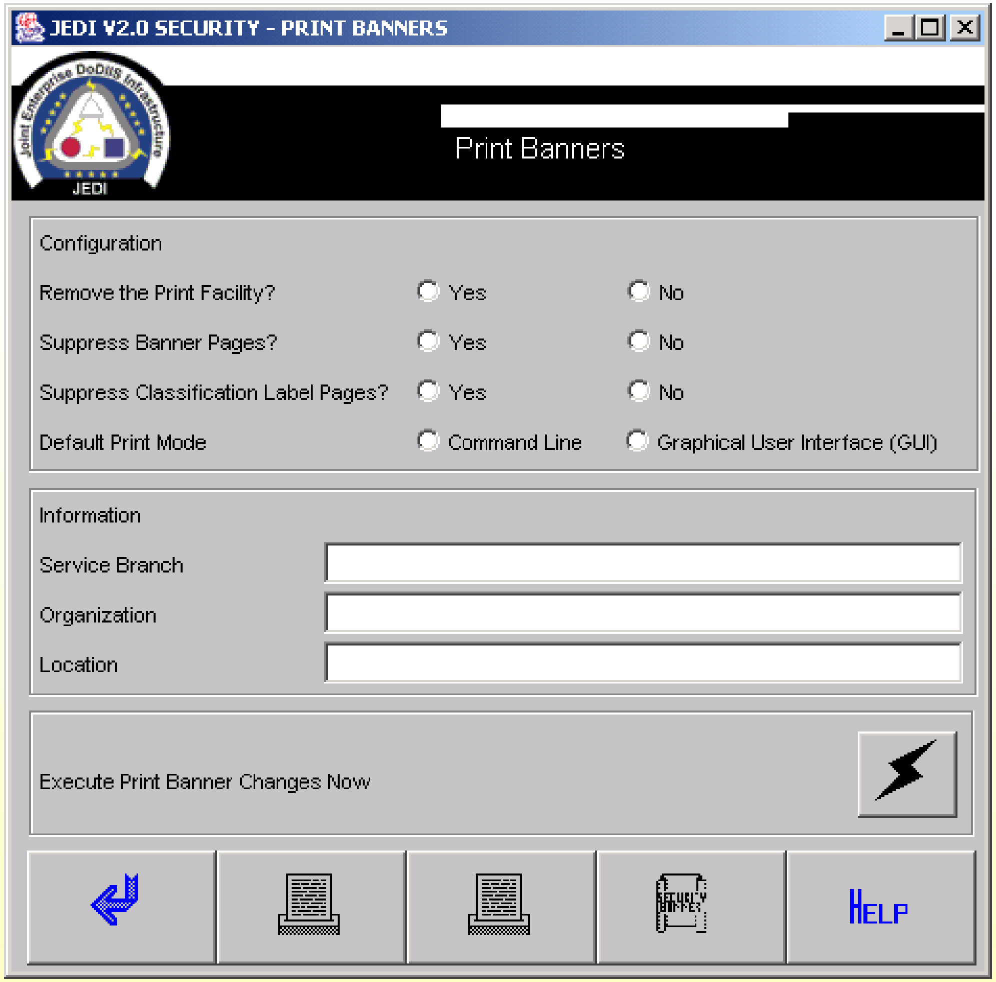
DNS Resolve

Execute Domain Name Service (DNS) Resolver Changes Now

Solaris 9 – JEDI PostInstallation



Solaris 9 – JEDI PostInstallation



JEDI V2.0 SECURITY - PRINT BANNERS

Print Banners

Configuration

Remove the Print Facility?	○ Yes	○ No
Suppress Banner Pages?	○ Yes	○ No
Suppress Classification Label Pages?	○ Yes	○ No
Default Print Mode	○ Command Line	○ Graphical User Interface (GUI)

Information

Service Branch

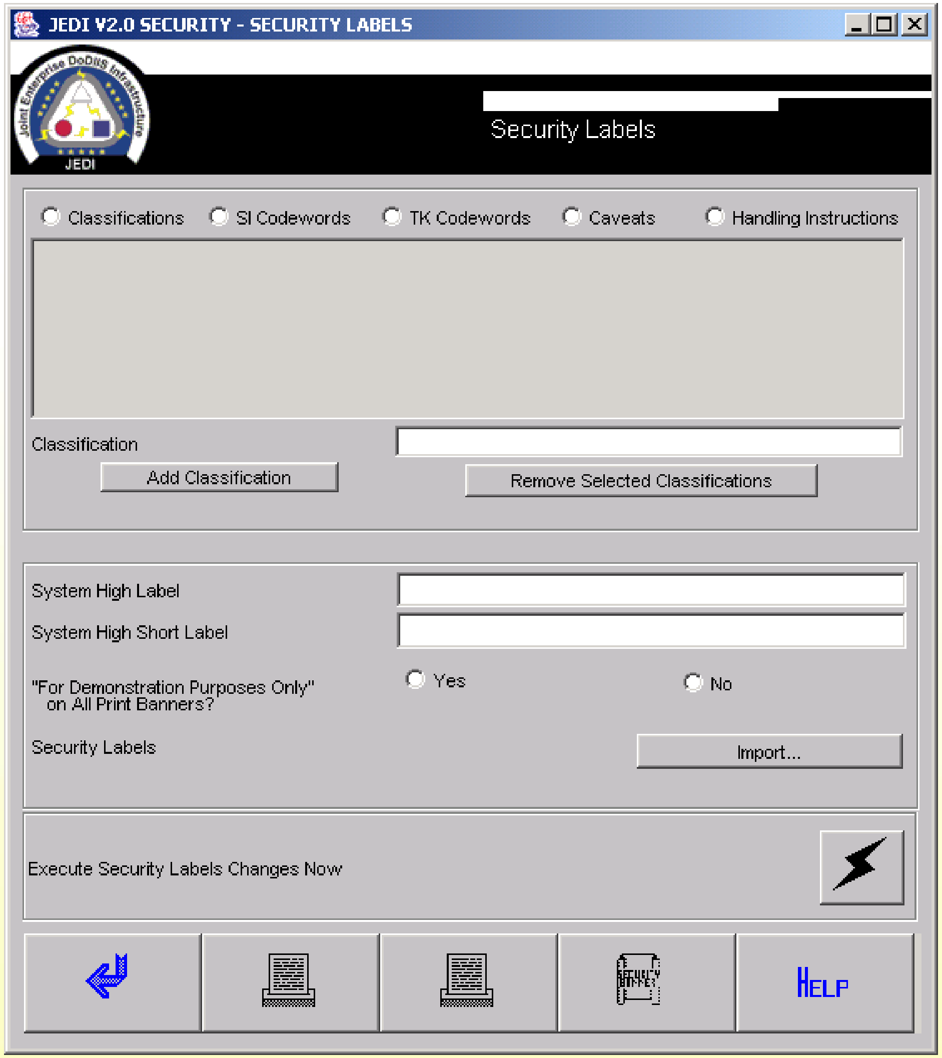
Organization

Location

Execute Print Banner Changes Now

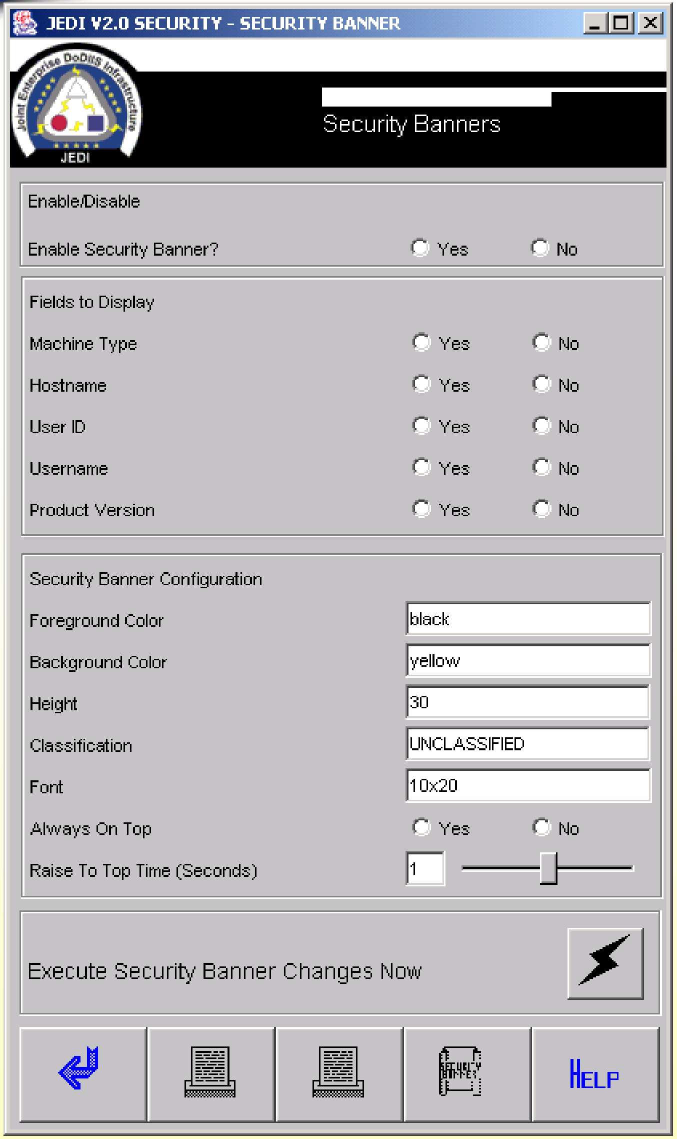
- **Print Banners**
  - Optional removal of JEDI Print Tool
  - Optional suppression of Banner Pages and Classification Labels
  - Sets Branch, Organization, and Location for Print Banner

Solaris 9 – JEDI PostInstallation



- **Security Labels**
  - Sets Classifications, Codeword, Caveats, and Handling Instructions for Printed Output
  - Not used for Trusted Solaris

Solaris 9 – JEDI PostInstallation


JEDI V2.0 SECURITY - SECURITY BANNER
Joint Enterprise DoDIIS Infrastructure
JEDI
Security Banners
HELP

Enable/Disable

Enable Security Banner?	○ Yes	○ No

Fields to Display

Machine Type	○ Yes	○ No
Hostname	○ Yes	○ No
User ID	○ Yes	○ No
Username	○ Yes	○ No
Product Version	○ Yes	○ No

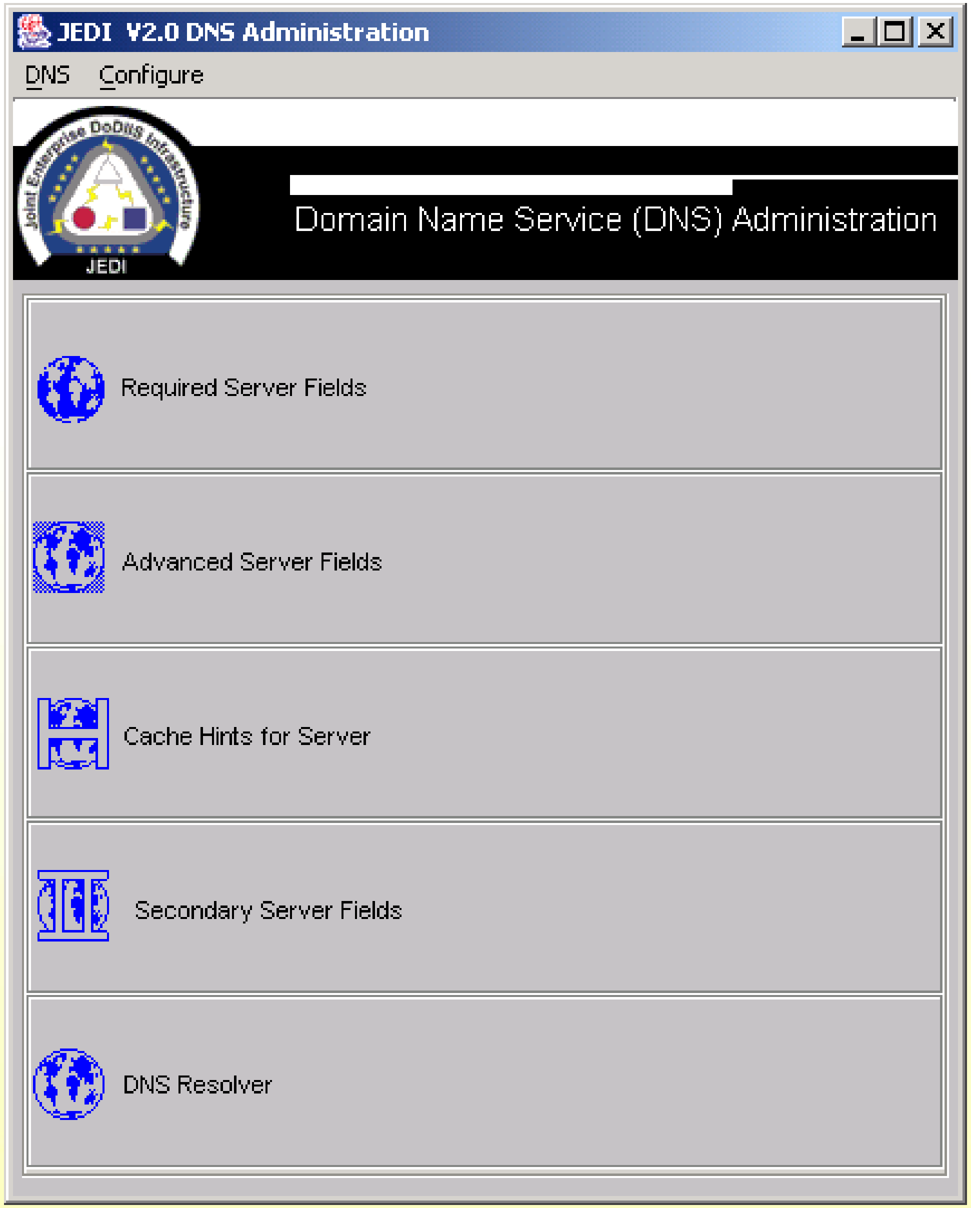
Security Banner Configuration

Foreground Color	black	
Background Color	yellow	
Height	30	
Classification	UNCLASSIFIED	
Font	10x20	
Always On Top	○ Yes	○ No
Raise To Top Time (Seconds)	1	

Execute Security Banner Changes Now

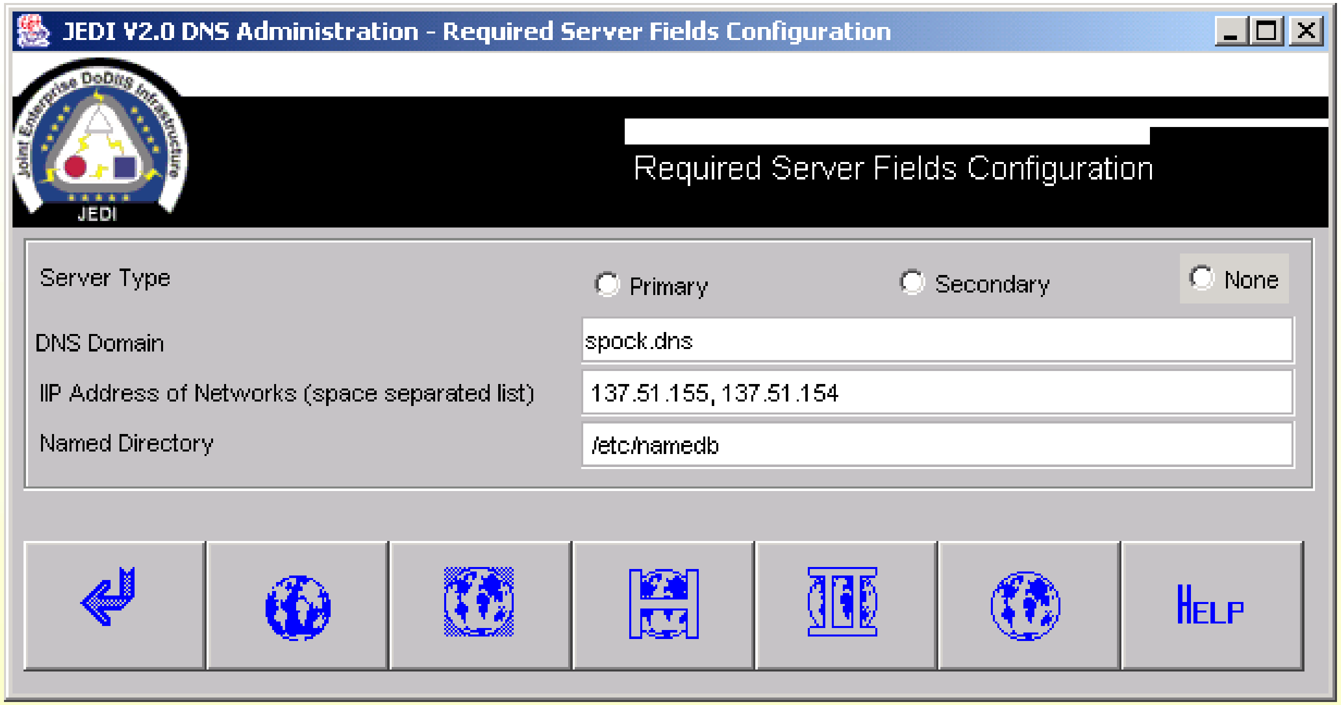
- **Security Banner**
  - Sets what to display on Banner
  - Configures Security Banner
  - Not used for Trusted Solaris

Solaris 9 – JEDI PostInstallation



Solaris 9 – JEDI PostInstallation

- **Required Server Fields Configuration**
  - Sets DNS domain and networks



JEDI V2.0 DNS Administration - Required Server Fields Configuration

Required Server Fields Configuration

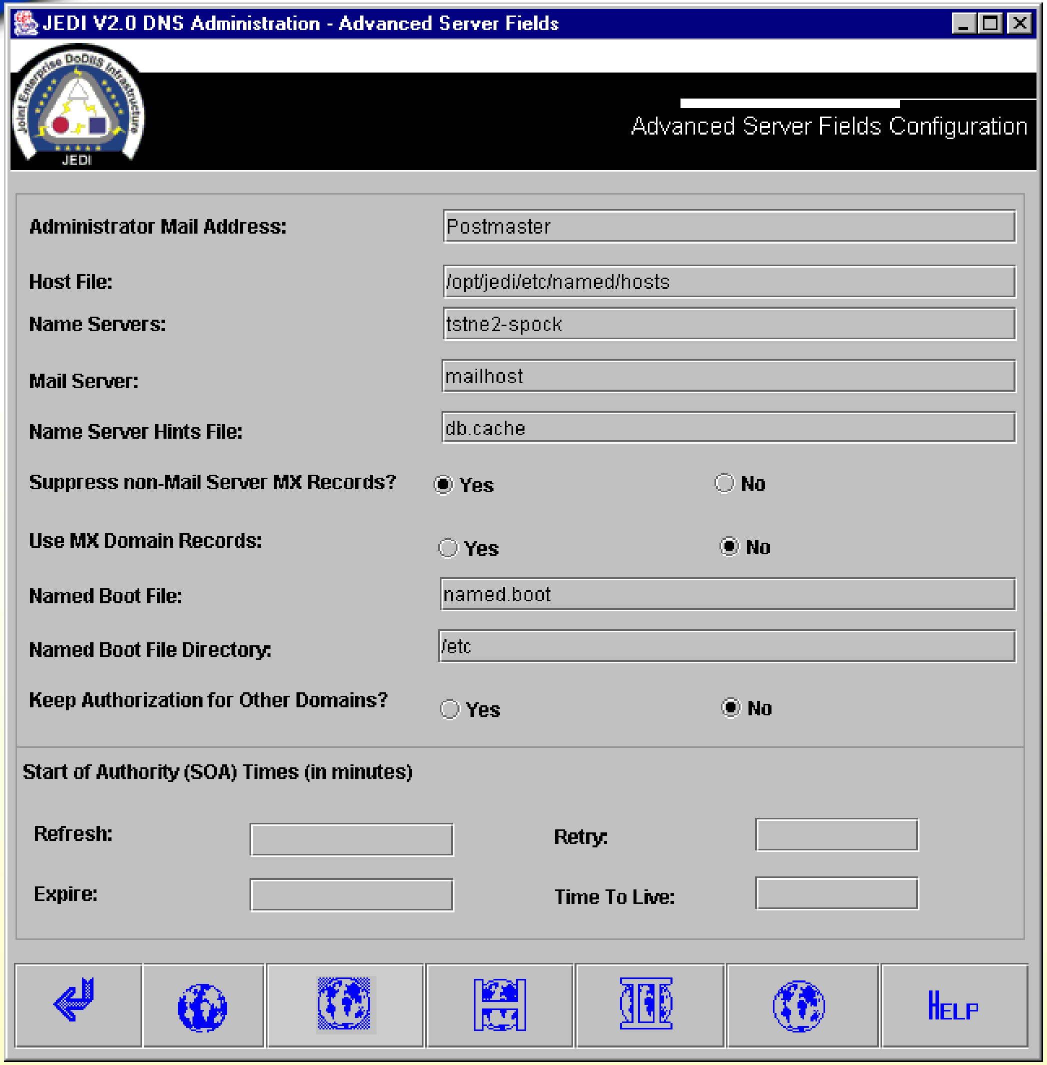
Server Type ○ Primary ○ Secondary ○ None

DNS Domain: spock.dns

IIP Address of Networks (space separated list): 137.51.155, 137.51.154

Named Directory: /etc/namedb

Solaris 9 – JEDI PostInstallation


JEDI V2.0 DNS Administration - Advanced Server Fields
Joint Enterprise DoDIIS Infrastructure
JEDI
HELP

Advanced Server Fields Configuration

Administrator Mail Address:	Postmaster	
Host File:	/opt/jedi/etc/named/hosts	
Name Servers:	tstne2-spock	
Mail Server:	mailhost	
Name Server Hints File:	db.cache	
Suppress non-Mail Server MX Records?	● Yes	○ No
Use MX Domain Records:	○ Yes	● No
Named Boot File:	named.boot	
Named Boot File Directory:	/etc	
Keep Authorization for Other Domains?	○ Yes	● No

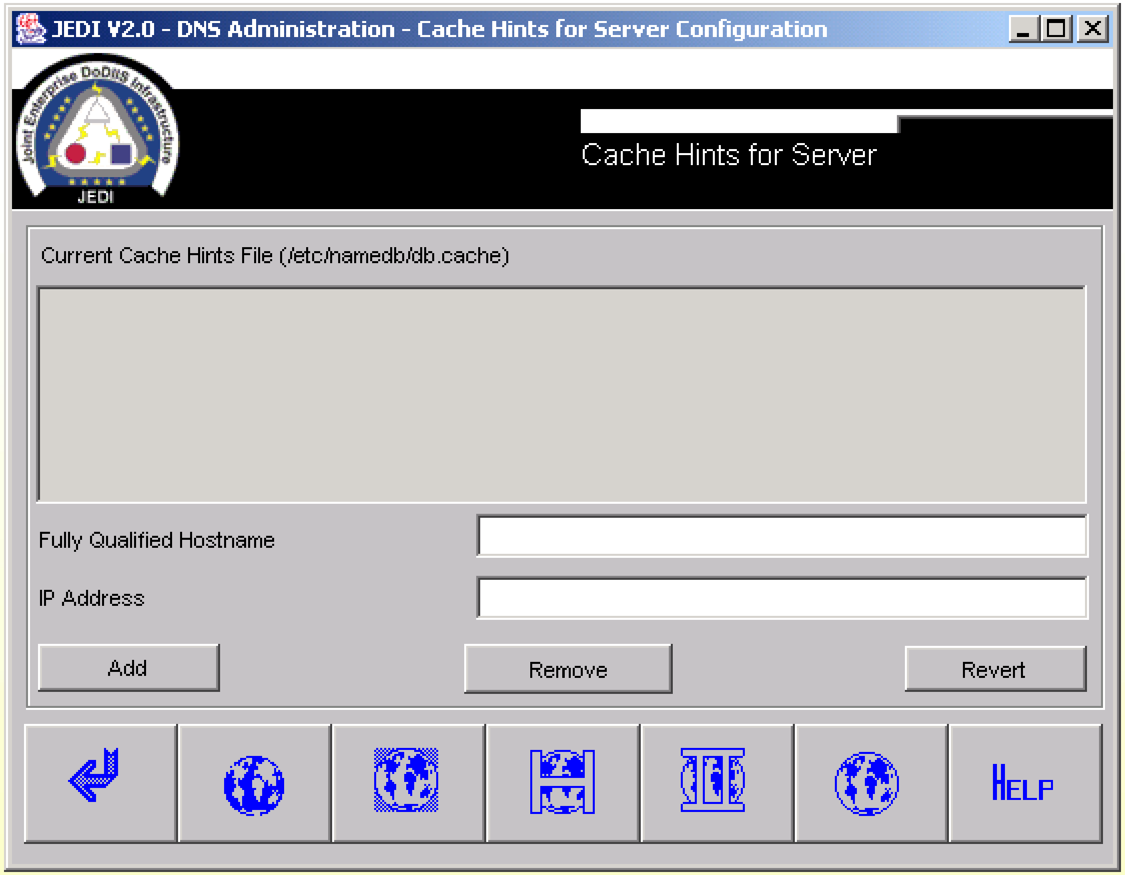
Start of Authority (SOA) Times (in minutes)

Refresh:		Retry:	
Expire:		Time To Live:	

- **Advanced Server Fields Configuration**
  - Sets advanced DNS Configuration settings

Solaris 9 – JEDI PostInstallation

- **Cache Hints**
  - Sets the location of Cache hints



JEDI V2.0 - DNS Administration - Cache Hints for Server Configuration

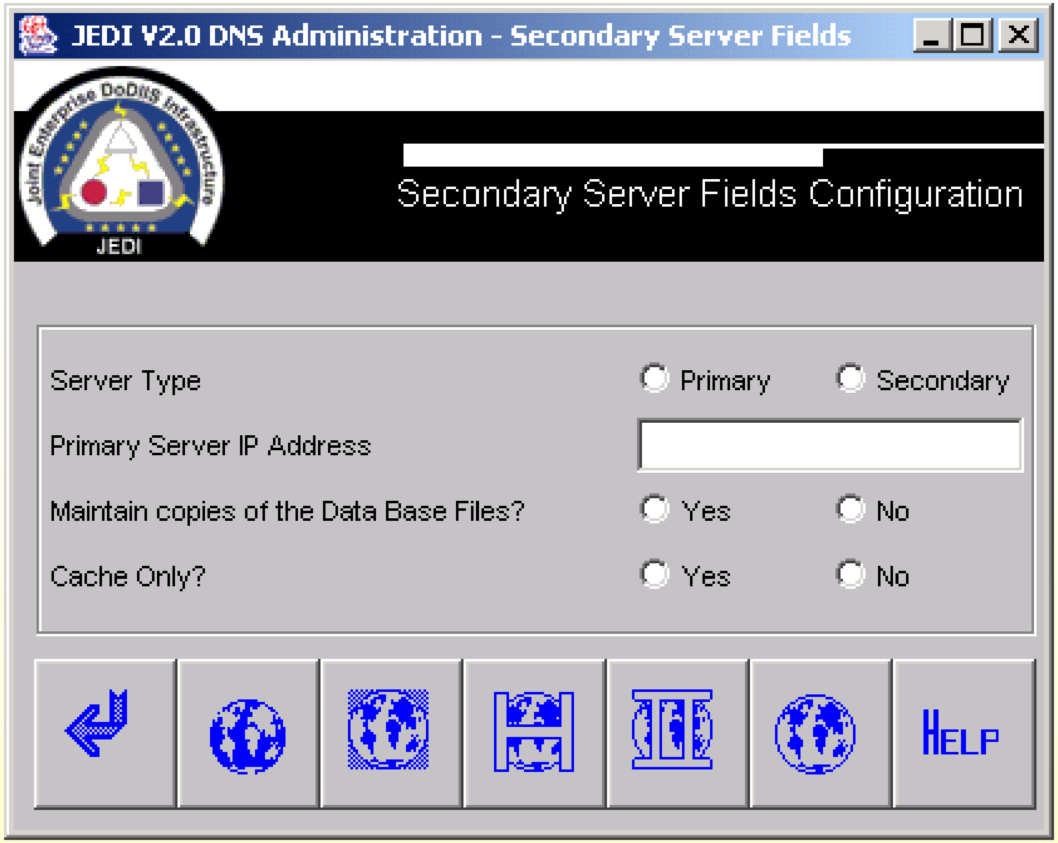
Cache Hints for Server

Current Cache Hints File (/etc/namedb/db.cache)

Fully Qualified Hostname

IP Address

Solaris 9 – JEDI PostInstallation



JEDI V2.0 DNS Administration - Secondary Server Fields

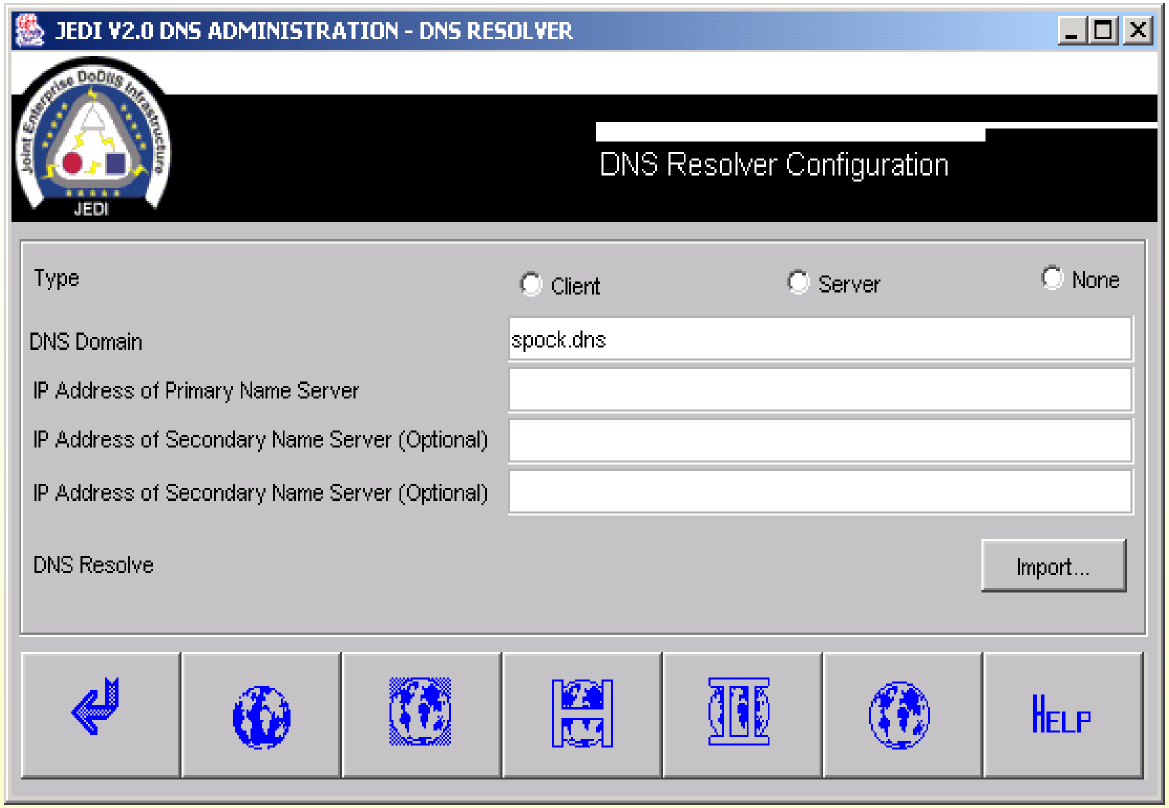
Secondary Server Fields Configuration

Server Type	○ Primary	○ Secondary
Primary Server IP Address		
Maintain copies of the Data Base Files?	○ Yes	○ No
Cache Only?	○ Yes	○ No

- **Secondary Server Fields**
  - Sets type of DNS server

Solaris 9 – JEDI PostInstallation

- **DNS Resolver Configuration**
  - Sets DNS Domain
  - Sets IP Address of Primary and Secondary Servers

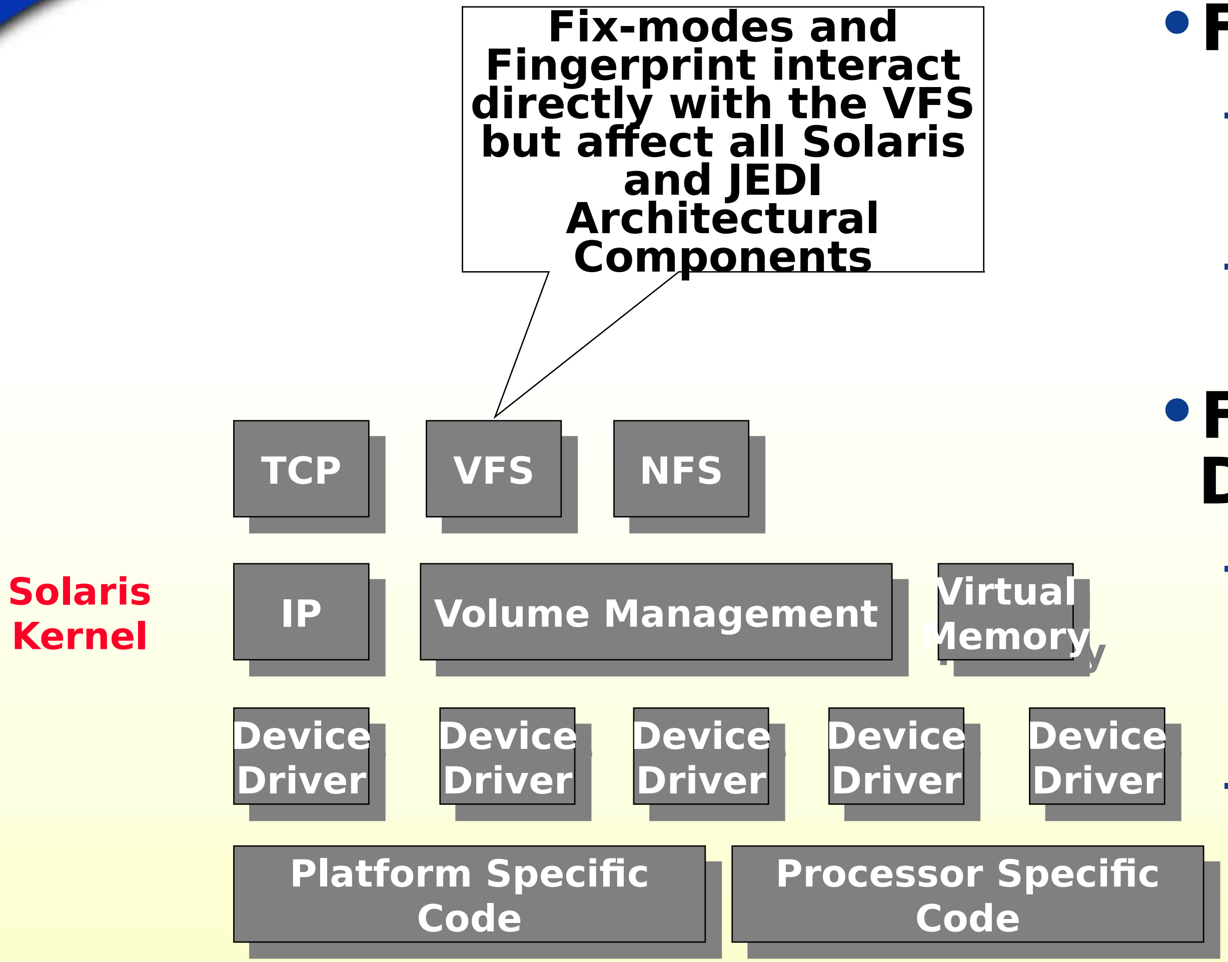


JEDI V2.0 DNS ADMINISTRATION - DNS RESOLVER

DNS Resolver Configuration

Type	○ Client ○ Server ○ None
DNS Domain	spock.dns
IP Address of Primary Name Server	
IP Address of Secondary Name Server (Optional)	
IP Address of Secondary Name Server (Optional)	
DNS Resolve	Import...

Solaris 9 – JEDI PostInstallation



Fix-modes and Fingerprint interact directly with the VFS but affect all Solaris and JEDI Architectural Components

Solaris Kernel

TCP

VFS

NFS

IP

Volume Management

Virtual Memory

Device Driver

Device Driver

Device Driver

Device Driver

Device Driver

Platform Specific Code

Processor Specific Code

- **Fix-modes**
  - Corrects modes on files
  - Executed during PostInstallation
- **Fingerprint Database**
  - Validates base Sun provided files
  - Installed during PostInstallation

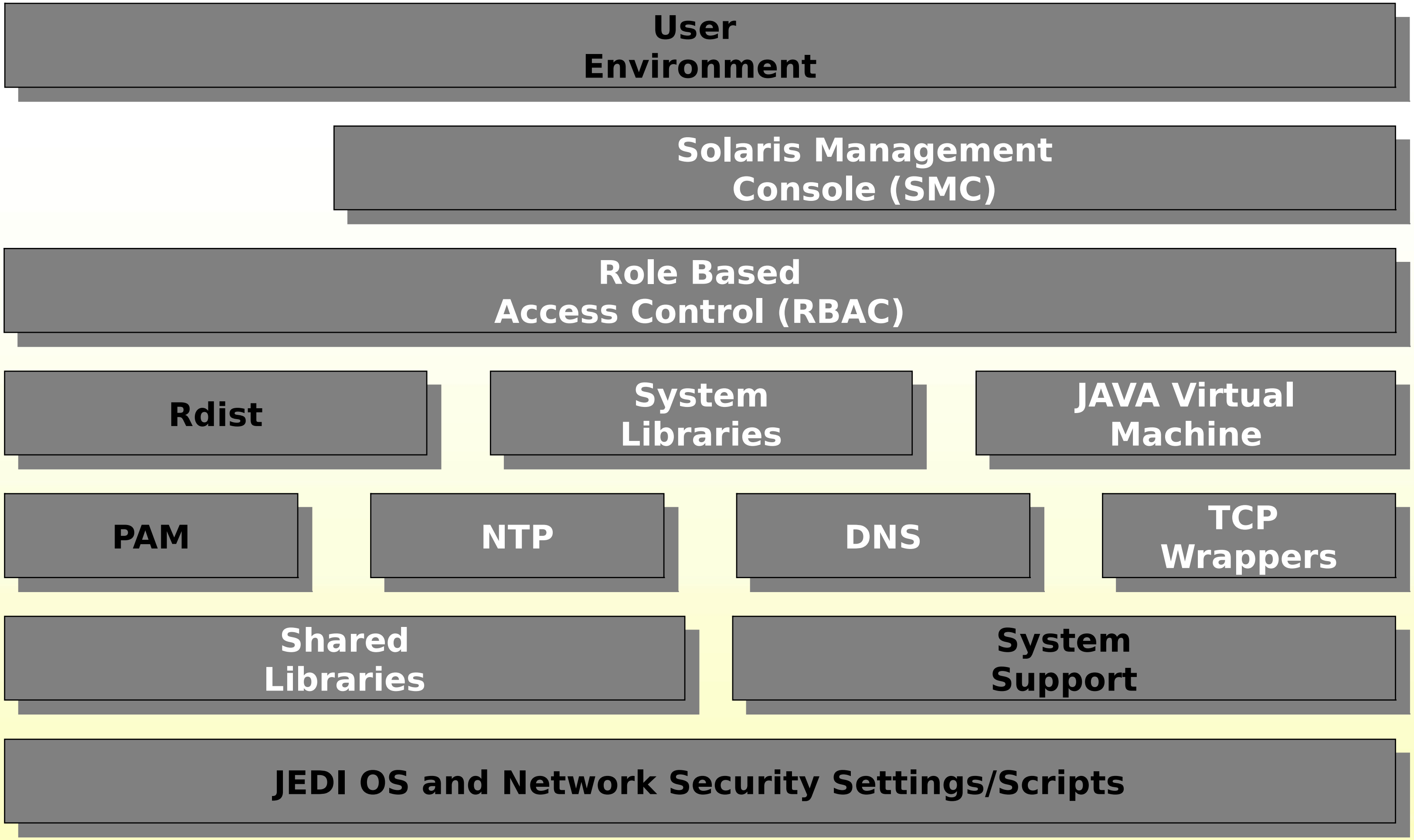
Solaris 9 - JEDI PostInstallation

- **During PostInstallation, JEDI 2.0 will**
  - Restrict NFS Server Requests to a privileged system port
    - /etc/system
      - Set nfssrv:nfs_portmon = 1
  - Prevent attempts to execute code on stacks
    - Restrict the ability to overwrite parts of the program stack of a privileged program
    - /etc/system
      - Set noexec_user_stack = 1
      - Set noexec_user_stack_log = 1
  - Use *coreadm* to
    - Store core files in /var/core
    - Generate a syslog message when a core file is created

NORTHROP GRUMMAN
Information Technology

Solaris 9 – JEDI PostInstallation

- **After PostInstallation, all Security Components are in place and configured**



User Environment

Solaris Management Console (SMC)

Role Based Access Control (RBAC)

Rdist

System Libraries

JAVA Virtual Machine

PAM

NTP

DNS

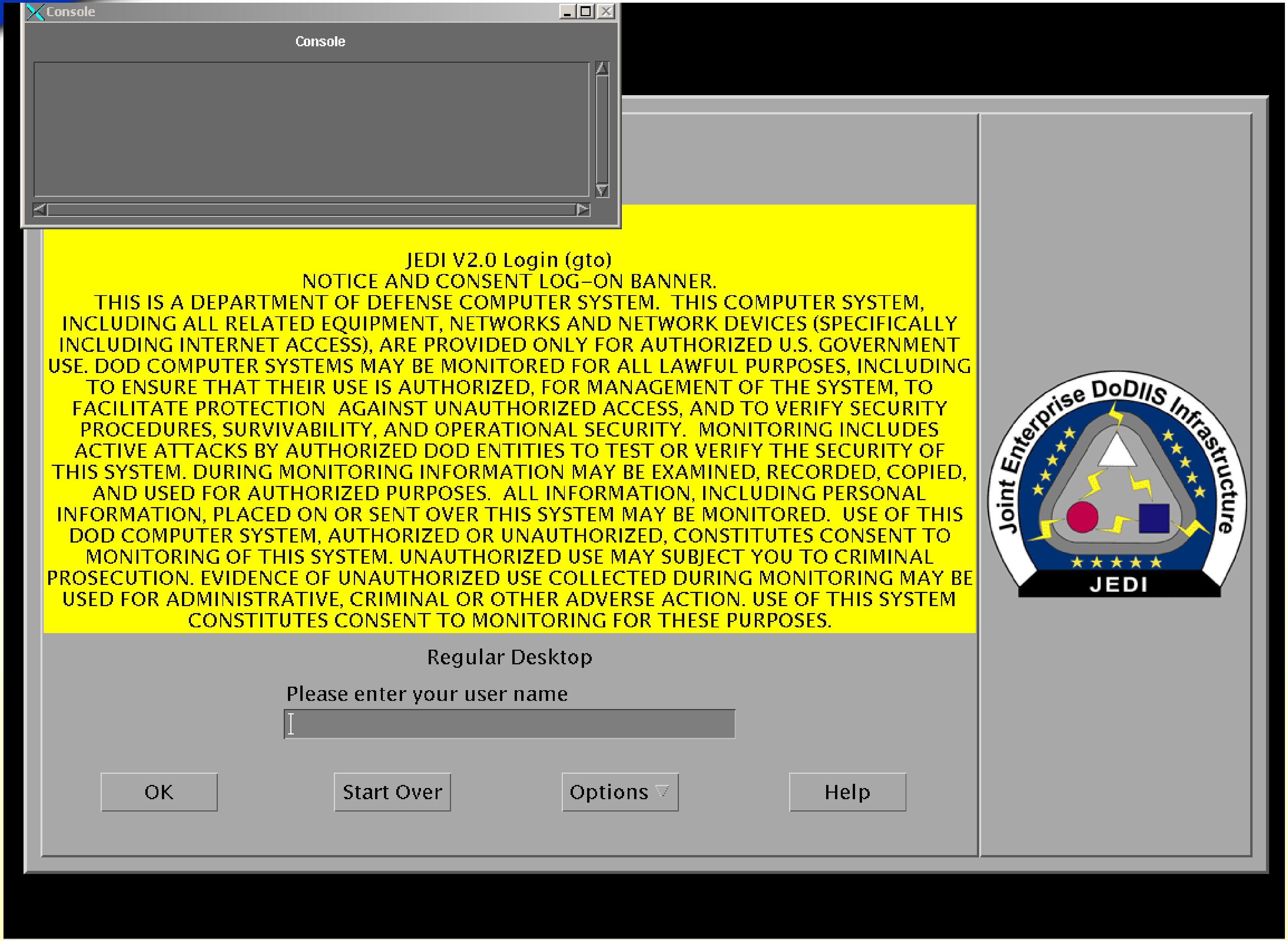
TCP Wrappers

Shared Libraries

System Support

JEDI OS and Network Security Settings/Scripts

Solaris 9 – JEDI User Environment

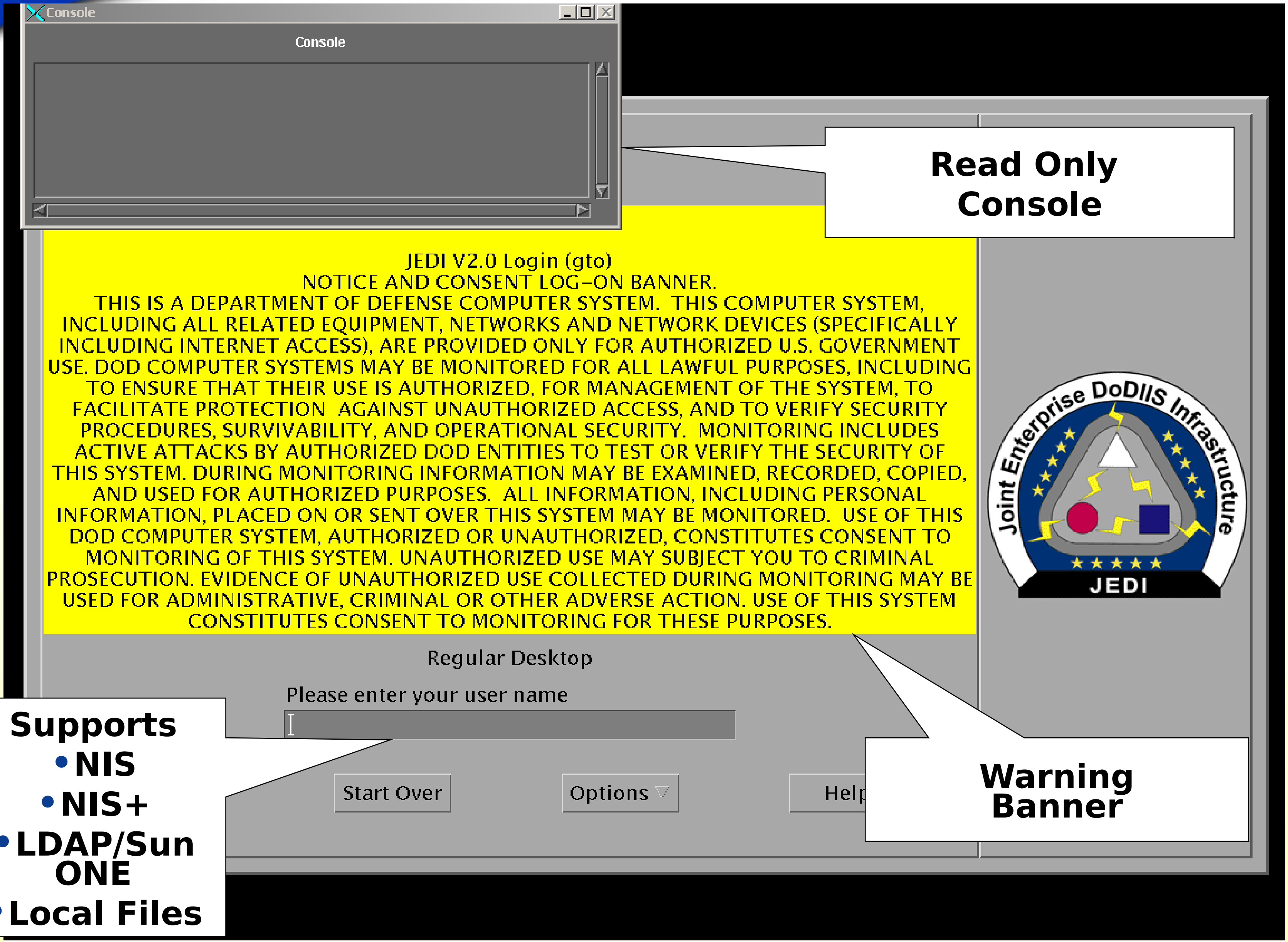


JEDI V2.0 Login (gto)
NOTICE AND CONSENT LOG-ON BANNER.
THIS IS A DEPARTMENT OF DEFENSE COMPUTER SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS AND NETWORK DEVICES (SPECIFICALLY INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DOD COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY, AND OPERATIONAL SECURITY. MONITORING INCLUDES ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING INFORMATION MAY BE EXAMINED, RECORDED, COPIED, AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED. USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES.

Regular Desktop

Please enter your user name

Solaris 9 – JEDI User Environment



JEDI V2.0 Login (gto)
NOTICE AND CONSENT LOG-ON BANNER.
THIS IS A DEPARTMENT OF DEFENSE COMPUTER SYSTEM. THIS COMPUTER SYSTEM, INCLUDING ALL RELATED EQUIPMENT, NETWORKS AND NETWORK DEVICES (SPECIFICALLY INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT USE. DOD COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING TO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO FACILITATE PROTECTION AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY PROCEDURES, SURVIVABILITY, AND OPERATIONAL SECURITY. MONITORING INCLUDES ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF THIS SYSTEM. DURING MONITORING INFORMATION MAY BE EXAMINED, RECORDED, COPIED, AND USED FOR AUTHORIZED PURPOSES. ALL INFORMATION, INCLUDING PERSONAL INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED. USE OF THIS DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE USED FOR ADMINISTRATIVE, CRIMINAL OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES.

Regular Desktop

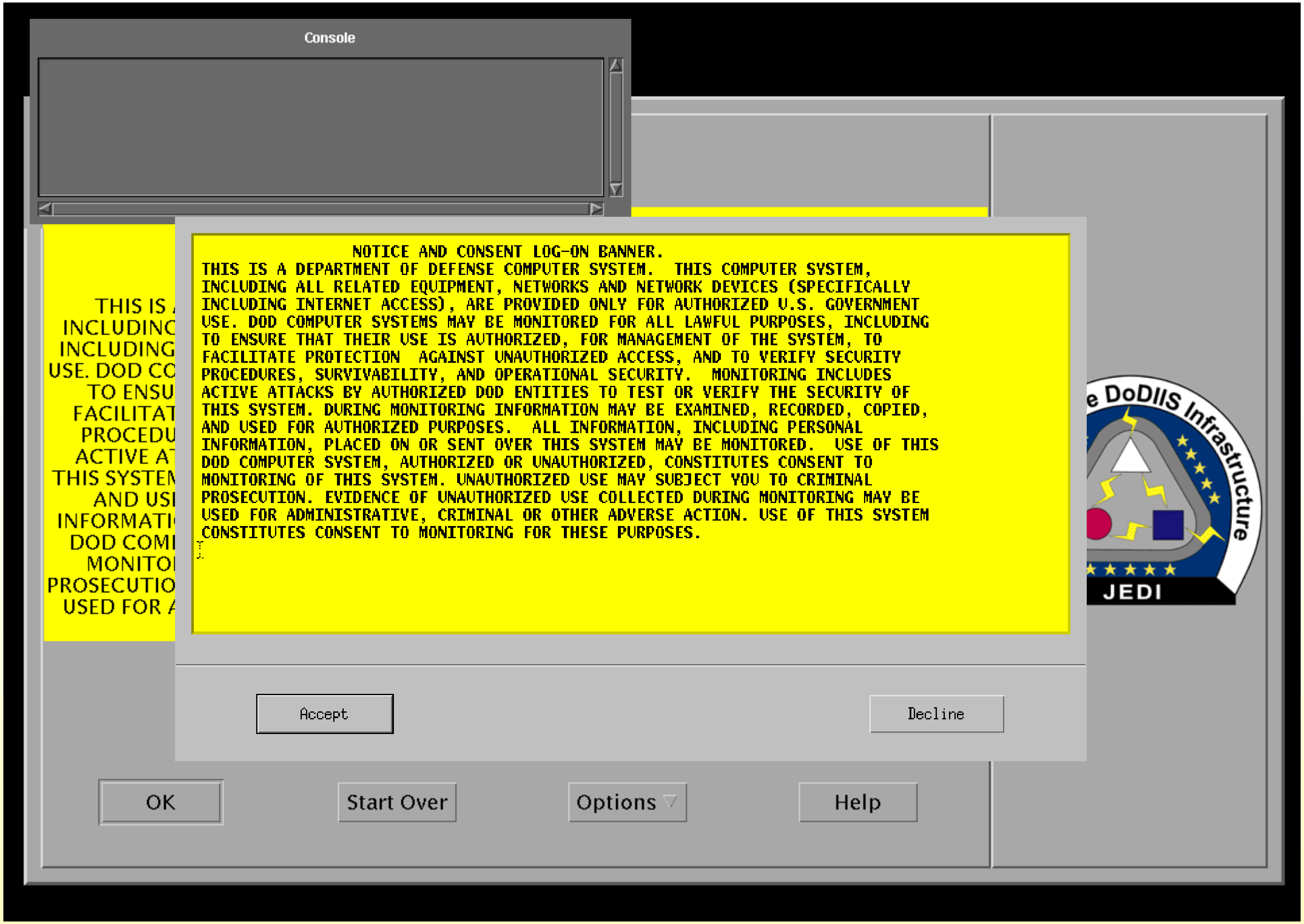
Please enter your user name

Read Only Console

Warning Banner

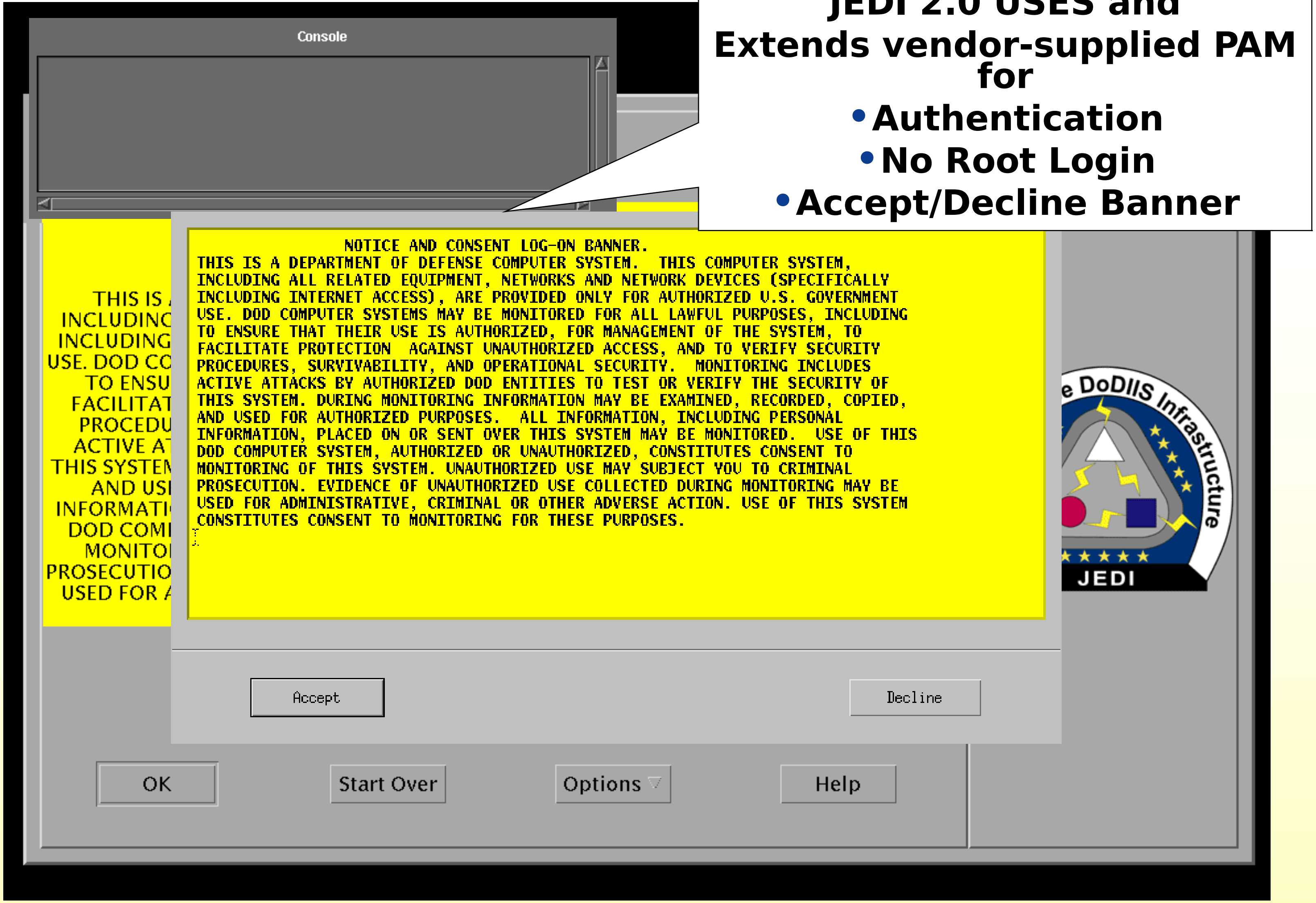
Supports
- **NIS**
- **NIS+**
- **LDAP/Sun ONE**
- **Local Files**

Solaris 9 – JEDI User Environment



```
                 NOTICE AND CONSENT LOG-ON BANNER.
THIS IS A DEPARTMENT OF DEFENSE COMPUTER SYSTEM.  THIS COMPUTER SYSTEM,
INCLUDING ALL RELATED EQUIPMENT, NETWORKS AND NETWORK DEVICES (SPECIFICALLY
INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT
USE. DOD COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING
TO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO
FACILITATE PROTECTION  AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY
PROCEDURES, SURVIVABILITY, AND OPERATIONAL SECURITY.  MONITORING INCLUDES
ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF
THIS SYSTEM. DURING MONITORING INFORMATION MAY BE EXAMINED, RECORDED, COPIED,
AND USED FOR AUTHORIZED PURPOSES.  ALL INFORMATION, INCLUDING PERSONAL
INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED.  USE OF THIS
DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO
MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL
PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE
USED FOR ADMINISTRATIVE, CRIMINAL OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM
CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES.
```

Solaris 9 – JEDI User Environment

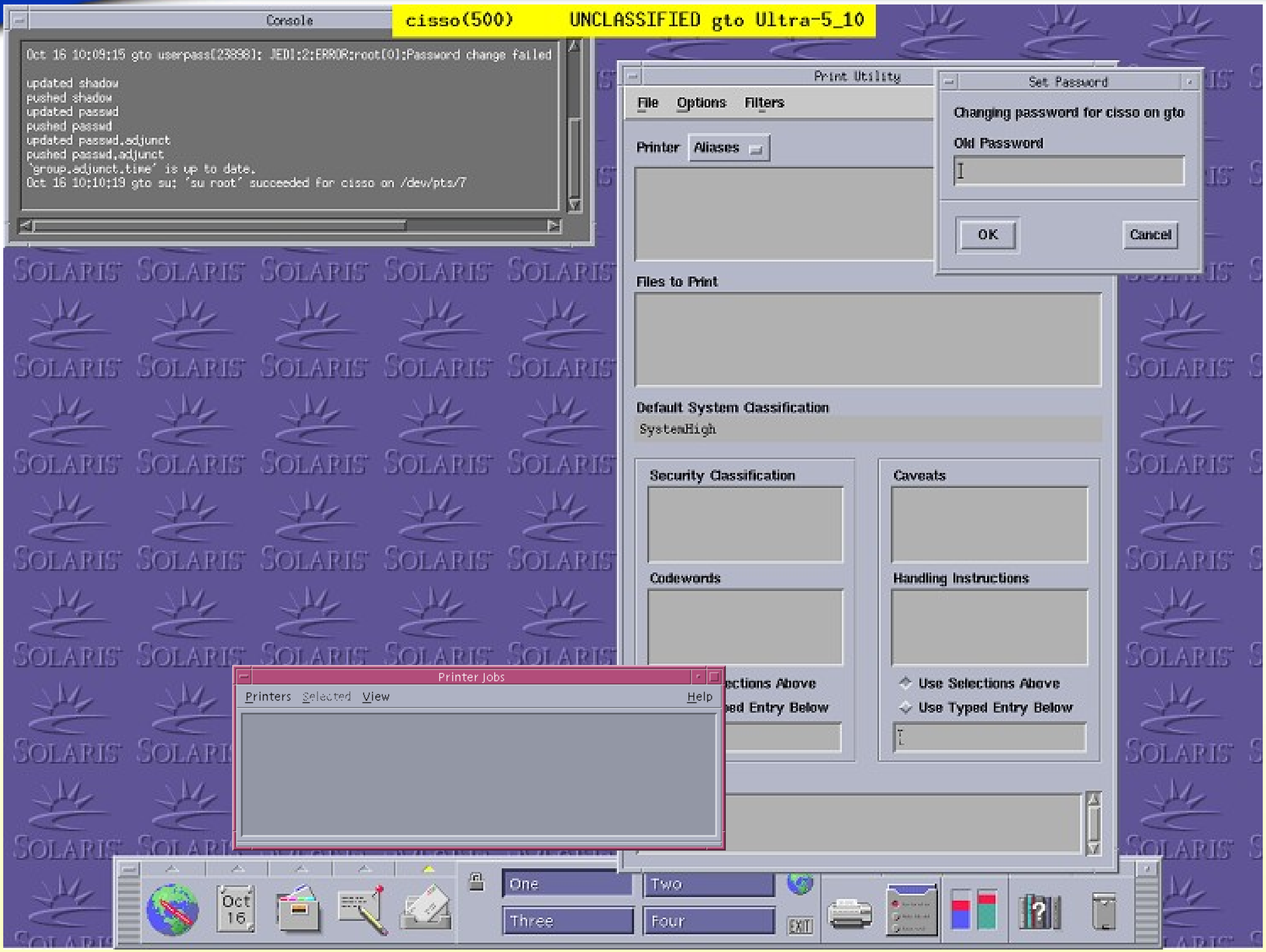


```
NOTICE AND CONSENT LOG-ON BANNER.
THIS IS A DEPARTMENT OF DEFENSE COMPUTER SYSTEM.  THIS COMPUTER SYSTEM,
INCLUDING ALL RELATED EQUIPMENT, NETWORKS AND NETWORK DEVICES (SPECIFICALLY
INCLUDING INTERNET ACCESS), ARE PROVIDED ONLY FOR AUTHORIZED U.S. GOVERNMENT
USE. DOD COMPUTER SYSTEMS MAY BE MONITORED FOR ALL LAWFUL PURPOSES, INCLUDING
TO ENSURE THAT THEIR USE IS AUTHORIZED, FOR MANAGEMENT OF THE SYSTEM, TO
FACILITATE PROTECTION  AGAINST UNAUTHORIZED ACCESS, AND TO VERIFY SECURITY
PROCEDURES, SURVIVABILITY, AND OPERATIONAL SECURITY.  MONITORING INCLUDES
ACTIVE ATTACKS BY AUTHORIZED DOD ENTITIES TO TEST OR VERIFY THE SECURITY OF
THIS SYSTEM. DURING MONITORING INFORMATION MAY BE EXAMINED, RECORDED, COPIED,
AND USED FOR AUTHORIZED PURPOSES.  ALL INFORMATION, INCLUDING PERSONAL
INFORMATION, PLACED ON OR SENT OVER THIS SYSTEM MAY BE MONITORED.  USE OF THIS
DOD COMPUTER SYSTEM, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO
MONITORING OF THIS SYSTEM. UNAUTHORIZED USE MAY SUBJECT YOU TO CRIMINAL
PROSECUTION. EVIDENCE OF UNAUTHORIZED USE COLLECTED DURING MONITORING MAY BE
USED FOR ADMINISTRATIVE, CRIMINAL OR OTHER ADVERSE ACTION. USE OF THIS SYSTEM
CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES.
```

JEDI 2.0 USES and Extends vendor-supplied PAM for

- **Authentication**
- **No Root Login**
- **Accept/Decline Banner**

Solaris 9 – JEDI User Environment



cisso(500) UNCLASSIFIED gto Ultra-5_10

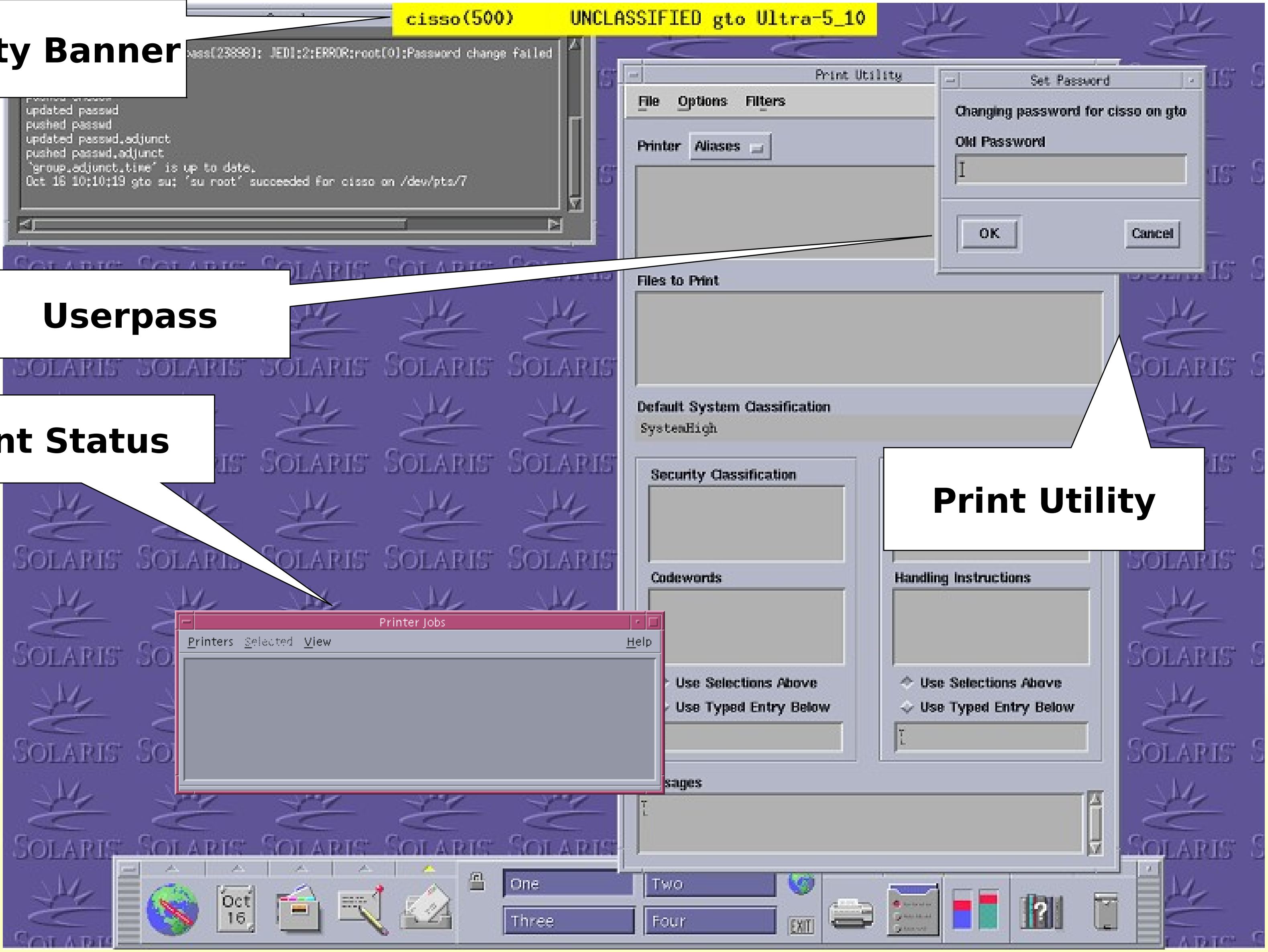
```
Oct 16 10:09:15 gto userpass[23898]: JEDI:2:ERROR:root[0]:Password change failed

updated shadow
pushed shadow
updated passwd
pushed passwd
updated passwd.adjunct
pushed passwd.adjunct
`group.adjunct.time' is up to date.
Oct 16 10:10:19 gto su: `su root' succeeded for cisso on /dev/pts/7
```

Changing password for cisso on gto

Old Password: I

Default System Classification: SystemHigh

Solaris 9 – JEDI User Environment



Security Banner

Userpass

Print Status

Print Utility

```
cisso(500)    UNCLASSIFIED gto Ultra-5_10
```

```
pass[23898]: JEDI:2:ERROR:root[0]:Password change failed
updated passwd
pushed passwd
updated passwd.adjunct
pushed passwd.adjunct
`group.adjunct.time' is up to date.
Oct 16 10:10:19 gto su: 'su root' succeeded for cisso on /dev/pts/7
```

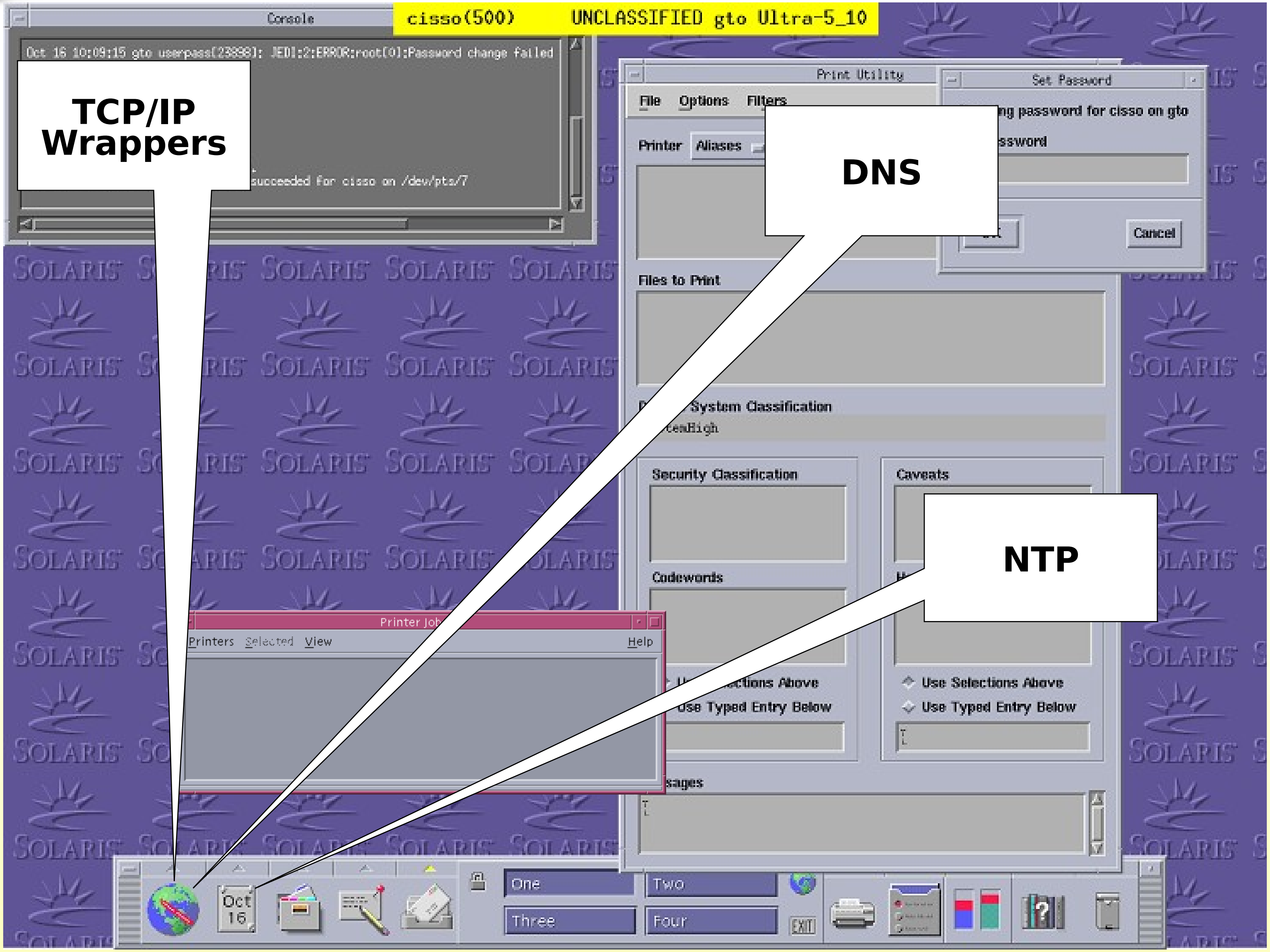
Changing password for cisso on gto

Old Password

Default System Classification

SystemHigh

Solaris 9 – JEDI User Environment



TCP/IP Wrappers

DNS

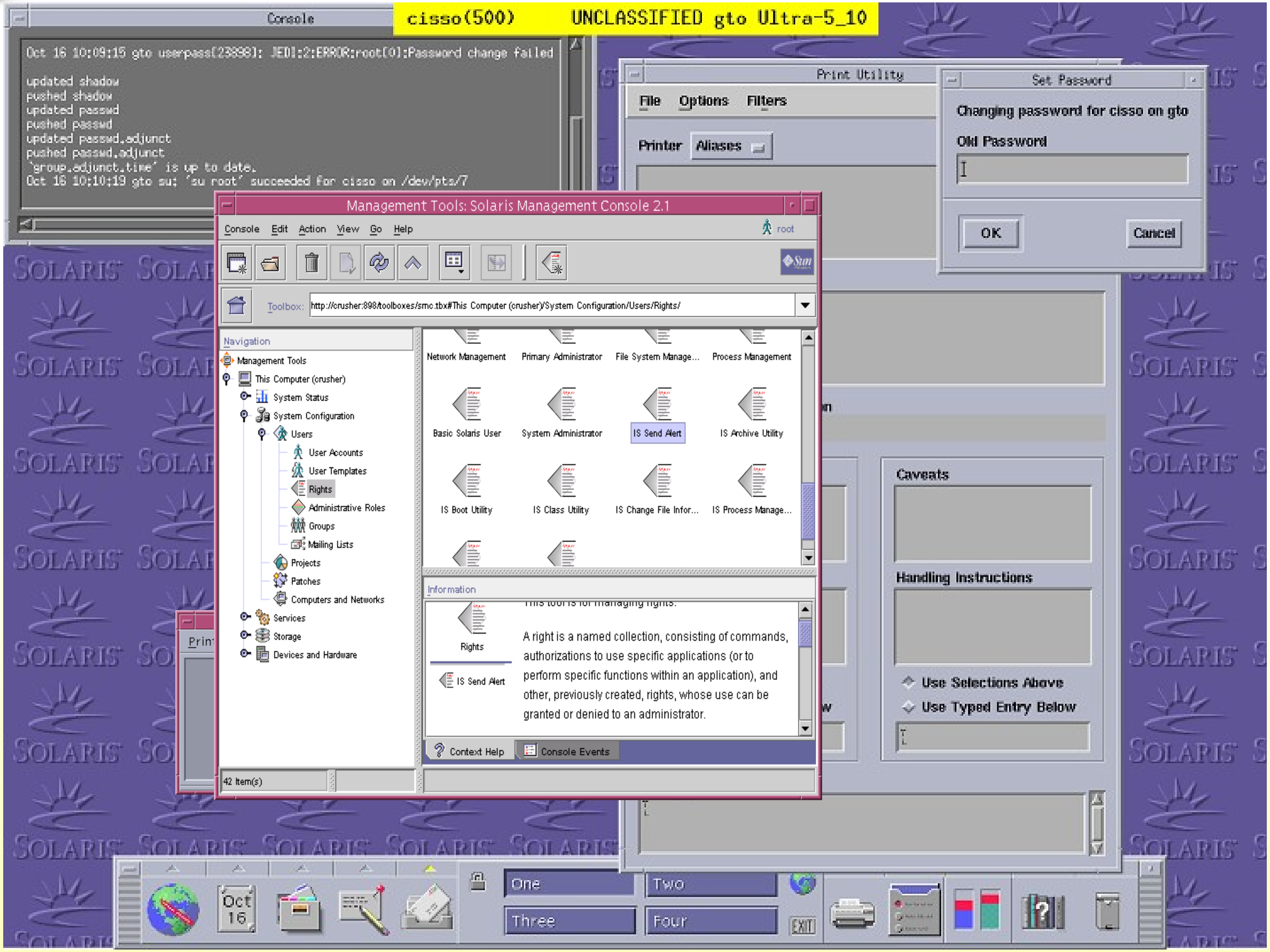
NTP

```
Oct 16 10:09:15 gto userpass[23898]: JEDI:2:ERROR:root[0]:Password change failed
succeeded for cisso on /dev/pts/7
```

cisso(500) UNCLASSIFIED gto Ultra-5_10

ng password for cisso on gto

Solaris 9 – JEDI/OE Security



cisso(500) UNCLASSIFIED gto Ultra-5_10

Console

```
Oct 16 10:09:15 gto userpass[23898]: JEDI:2:ERROR:root[0]:Password change failed

updated shadow
pushed shadow
updated passwd
pushed passwd
updated passwd.adjunct
pushed passwd.adjunct
`group.adjunct.time' is up to date.
Oct 16 10:10:19 gto su: 'su root' succeeded for cisso on /dev/pts/7
```

Set Password

Changing password for cisso on gto

Old Password

Management Tools: Solaris Management Console 2.1

Toolbox: http://crusher:898/toolboxes/smc.tbx#This Computer (crusher)/System Configuration/Users/Rights/

Information

This tool is for managing rights.

A right is a named collection, consisting of commands, authorizations to use specific applications (or to perform specific functions within an application), and other, previously created, rights, whose use can be granted or denied to an administrator.

42 item(s)

Roadmap

- **Solaris 9 Public Design Review**
  - JEDI 2.0 Requirements
  - Support for Solaris 9
  - ➡ Transition JEDI Tools to Role Based Access Control
  - Transition JEDI Tools to Solaris Management Console
  - Removing Dependency on JEDI Maps
  - Secure Shell
  - JASS Interface
  - Pluggable Authentication Modules
  - Flash Archive Support
  - Optional SASF for Solaris 9
  - Integration of ISS into JEDI 2.0 Baseline
  - Additional Recommendations

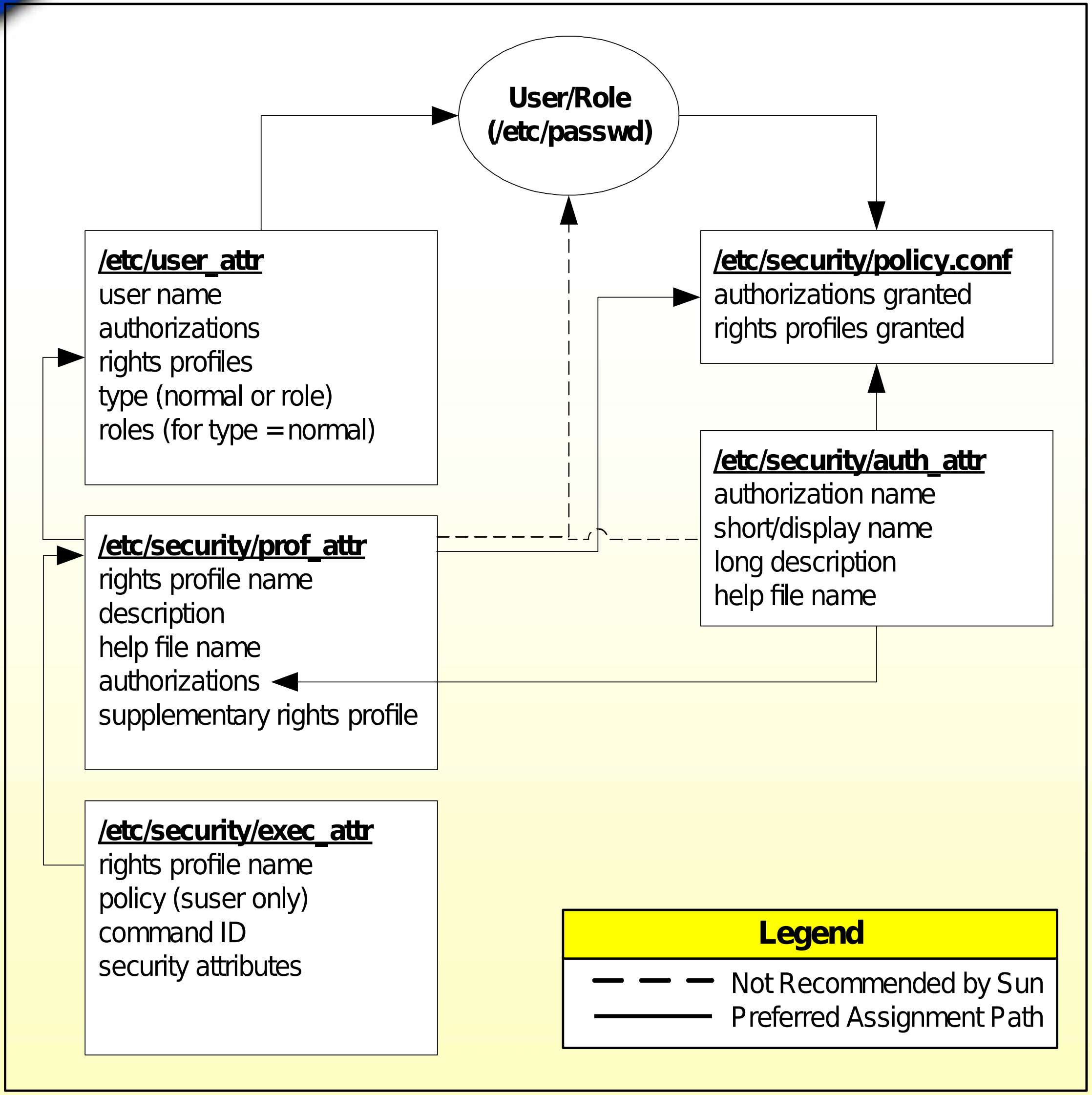
Roadmap - RBAC

- Transition JEDI Tools to Role Based Access Control
  - Features
  - Overview
  - Maintenance
    - Authorizations
    - Rights Profiles
    - Roles
  - Current JEDI TFM flow
  - New Process flow
  - Design Issues

Role Based Access Control (RBAC)

- **RBAC provides a fine-grained mechanism for managing the rights and authorizations of users and roles. Features of RBAC include:**
  - Available starting in Solaris 8
  - Authentication databases can be supported using NIS, NIS+, LDAP, or files
  - Administrators can create unlimited number of roles
  - User can belong to multiple roles
  - System supplied Application Programming Interfaces (API) which support C/C++, Java, and Shell Scripts
  - Integrated in with Sun's C2 audits
  - A vendor-supplied interface for maintaining Roles and Rights Profiles

RBAC - Overview



User/Role
(/etc/passwd)

/etc/user_attr
user name
authorizations
rights profiles
type (normal or role)
roles (for type = normal)

/etc/security/policy.conf
authorizations granted
rights profiles granted

/etc/security/auth_attr
authorization name
short/display name
long description
help file name

/etc/security/prof_attr
rights profile name
description
help file name
authorizations
supplementary rights profile

/etc/security/exec_attr
rights profile name
policy (suser only)
command ID
security attributes

Legend	
— — —	Not Recommended by Sun
——	Preferred Assignment Path

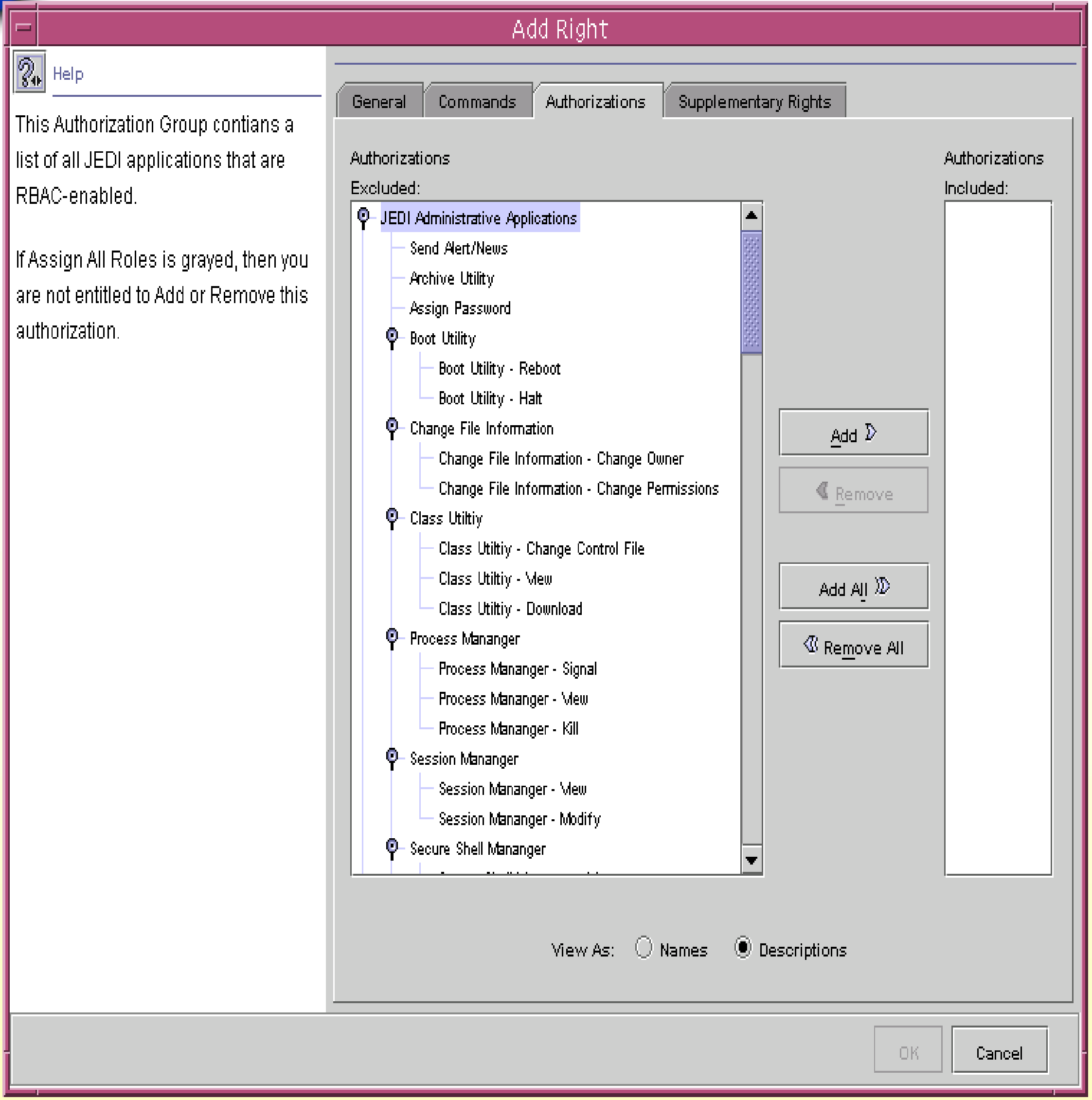
- **RBAC database files include**
  - /etc/user_attr
  - /etc/security/auth_attr
  - /etc/security/prof_attr
  - /etc/security/policy.conf
  - /etc/security/exec_attr

- **These files allow a user to be associated with a specified authorization by**
  - Assigning an authorization to a rights profile, the rights profile to a role, the role with a user (Preferred)
  - Assigning an authorization to a rights profile, and the rights profile to the user
  - Assigning an authorization directly to the user

RBAC – Maintenance

- **RBAC uses 5 files to maintain authorizations and which users/roles have access to those authorizations. These files will be maintained as follows:**
  - **auth_attr**
    - Initially configured – During JEDI installation
    - Maintained – Not required
  - **prof_attr**
    - Initially configured – During JEDI installation
    - Maintained – Vendor-supplied interface
  - **user_attr**
    - Initially configured – During JEDI installation
    - Maintained – Vendor-supplied interface
  - **exec_attr**
    - No plans to configure or maintain for JEDI applications
  - **policy.conf**
    - No plans to configure or maintain for JEDI applications

RBAC – Authorizations



This Authorization Group contians a list of all JEDI applications that are RBAC-enabled.

If Assign All Roles is grayed, then you are not entitled to Add or Remove this authorization.

Authorizations Excluded:

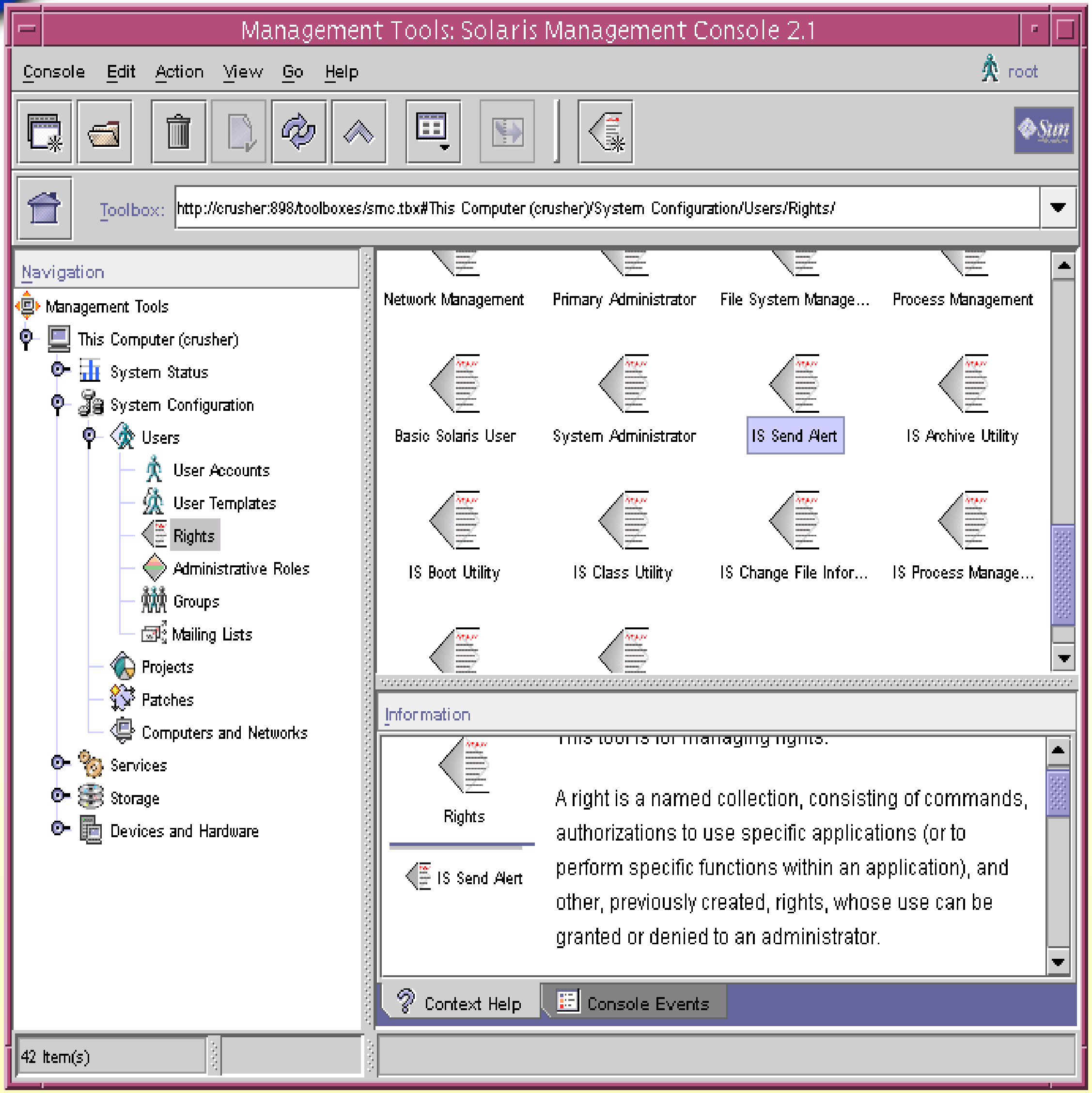
- JEDI Administrative Applications
  - Send Alert/News
  - Archive Utility
  - Assign Password
  - Boot Utility
    - Boot Utility - Reboot
    - Boot Utility - Halt
  - Change File Information
    - Change File Information - Change Owner
    - Change File Information - Change Permissions
  - Class Utitiy
    - Class Utitiy - Change Control File
    - Class Utitiy - View
    - Class Utitiy - Download
  - Process Mananger
    - Process Mananger - Signal
    - Process Mananger - View
    - Process Mananger - Kill
  - Session Mananger
    - Session Mananger - View
    - Session Mananger - Modify
  - Secure Shell Mananger

Authorizations Included:

View As: ○ Names ● Descriptions

- /etc/security/auth_attr
  - Defines “Authorization Strings”
  - Updated during the JEDI installation to include the default JEDI “Authorization Strings”
  - Does not require maintenance after the JEDI installation
  - Added to a Rights

RBAC – Rights Profile

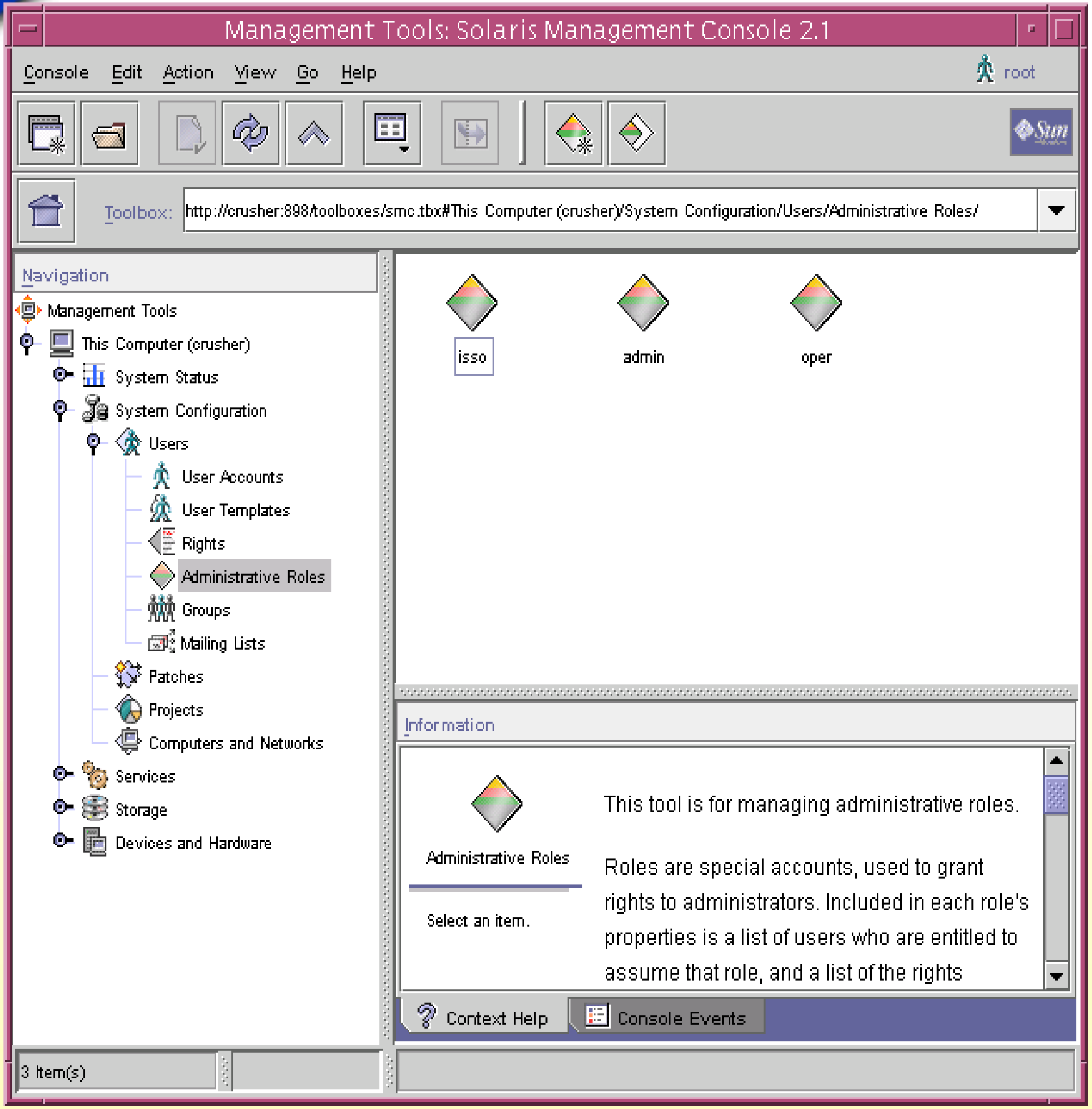


This tool is for managing rights.

A right is a named collection, consisting of commands, authorizations to use specific applications (or to perform specific functions within an application), and other, previously created, rights, whose use can be granted or denied to an administrator.

- /etc/security/prof_attr
  - Defines Rights Profiles
  - Updated during the JEDI installation to include the default JEDI Rights Profiles
  - There will be one Rights Profile entry for each unique JEDI Authorization String
  - Maintained using

RBAC – Administrative Roles



Toolbox: http://crusher:898/toolboxes/smc.tbx#This Computer (crusher)/System Configuration/Users/Administrative Roles/

Select an item.

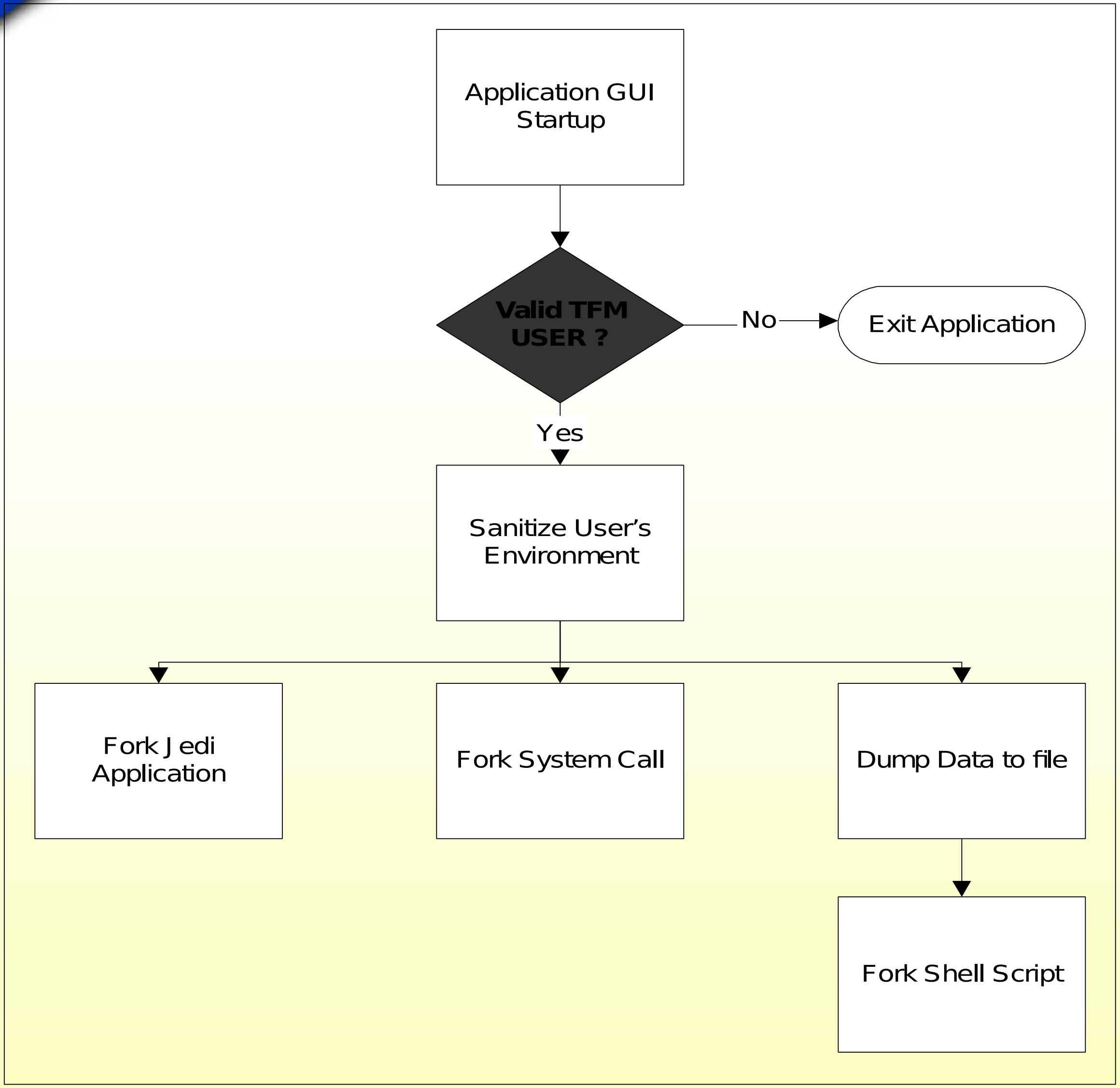
This tool is for managing administrative roles.

Roles are special accounts, used to grant rights to administrators. Included in each role's properties is a list of users who are entitled to assume that role, and a list of the rights

- **/etc/user_attr**
  - Defines Roles and identify which user have access to those roles
  - Updated during the JEDI installation to allow the user to install the Default JEDI roles or to create a custom Role
  - Maintained using the Vendor-supplied Administrative Roles Interface

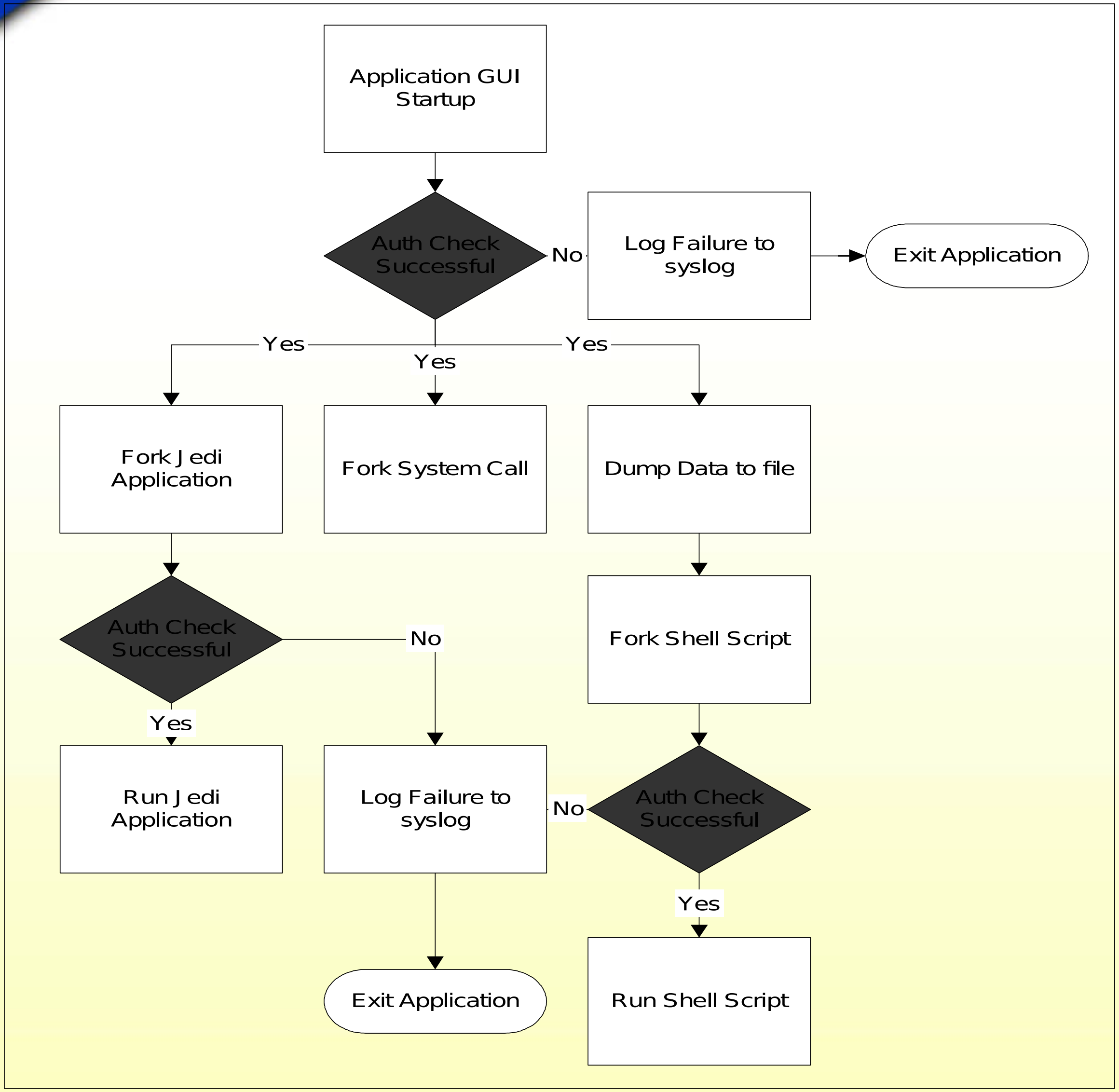
NORTHROP GRUMMAN
Information Technology

RBAC – Current Process Flow



- **Current Applications**
  - Use the verify_tfm_user function call
  - Generates a warning message on failure
  - Sanitizes a users environment
  - Provides all-or-nothing access to an application

RBAC – New Process Flow



- **Modified Applications will**
  - Use the vendor-supplied API(s) to determine if a user has a specified authorization
  - Generates a warning message on failure
  - Have the ability to provide a more granular authorization check

RBAC - Design Issues

- The current RBAC functionality provided by JEDI will sanitize a users environment, based on a configuration file, once a user has been validated. This is functionality that may not be re-created using Solaris's RBAC. With Solaris's RBAC, a role is nothing more than a specialized group. It is possible to control a role's environment by creating a profile for this group.
- With JEDI, a user can belong to one or more trusted roles, and have the ability to invoke more than one role at a time. With Solaris's RBAC, a user can belong to more than one role, but can only assume one role at a time.
- A profile/right may be assigned directly to a user. As a result, a user could make inadvertent mistakes by misuse of their privileges. This practice is discouraged by Sun.
- Since roles are implemented as a form of specialized user, all normal users who assume a specified role have access to that role's home directory, have access to the same files, and operate in the same environment.
- RBAC supports the locale variable. This allows the developer to create help files in different languages. Currently, we are only creating help files in English.

Roadmap

- **Solaris 9 Public Design Review**
  - JEDI 2.0 Requirements
  - Support for Solaris 9
  - Transition JEDI Tools to Role Based Access Control
  - Transition JEDI Tools to Solaris Management Console
  - Removing Dependency on JEDI Maps
  - Secure Shell
  - JASS Interface
  - Pluggable Authentication Modules
  - Flash Archive Support
  - Optional SASF for Solaris 9
  - Integration of ISS into JEDI 2.0 Baseline
  - Additional Recommendations

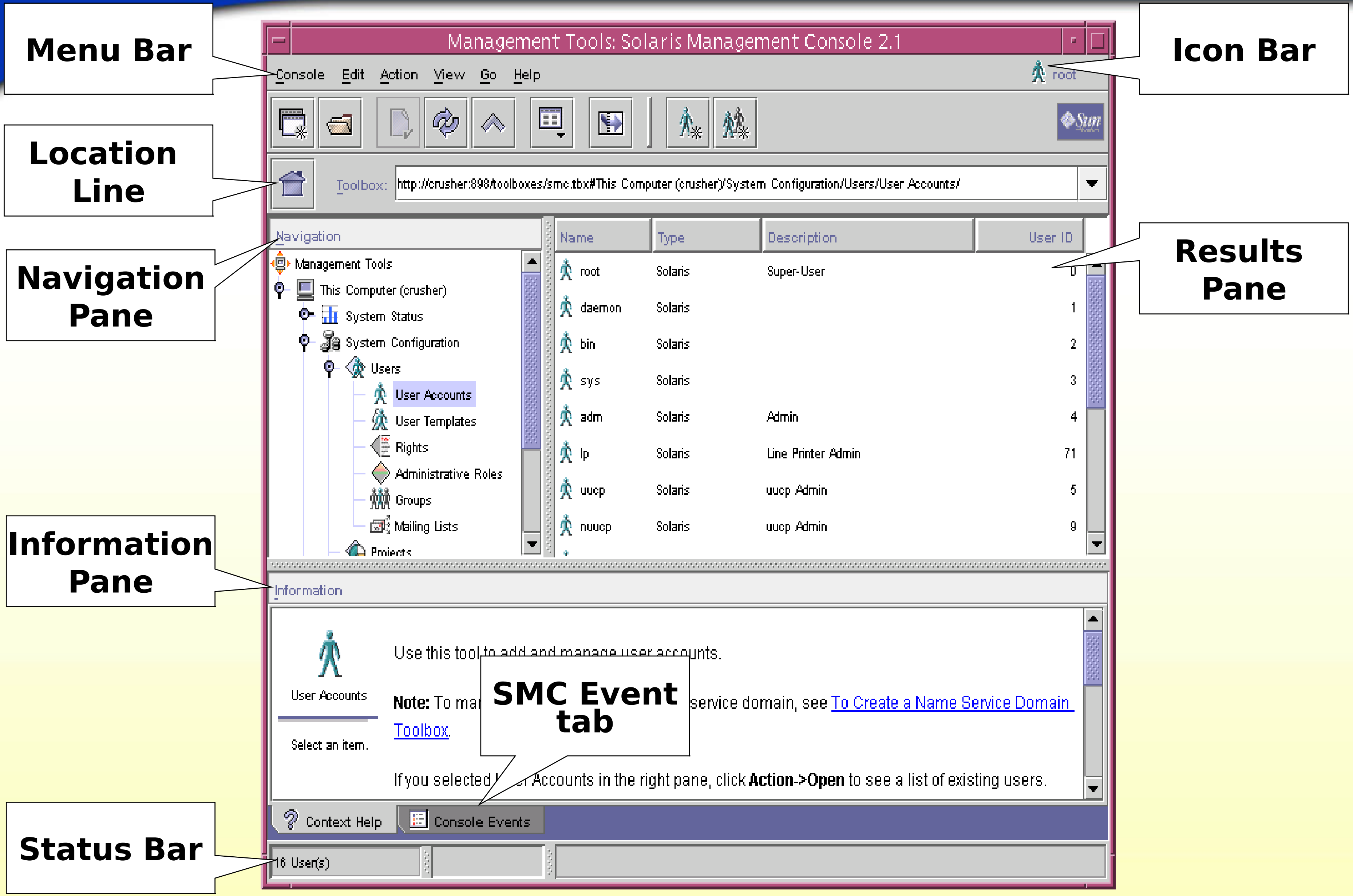
Roadmap - SMC

- Transition JEDI Tools to Solaris Management Console
  - Overview
  - Applications Requirements
  - Transitioned Applications
  - COTS Migration
  - Legacy Applications
  - Deprecated Applications

Solaris Management Console (SMC)

- **This is not Sun’s Management Center**
- **SMC is a graphical user interface that provides access to Solaris System Administration tools**
- **SMC provides**
  - Support for Java 1.4 (for Solaris 9) and Java 1.3 (for Trusted Solaris 8)
  - Toolboxes to group administrative applications
  - Support for C2 Audits
  - A group of core services:
    - Authentication
    - Authorization
    - Logging
    - User Preferences
    - Persistence
    - Messaging
    - Application launch management
  - Management Scope which includes
    - Files
    - LDAP
    - NIS
    - NIS+
    - DNS

SMC – Main Window Overview



http://crusher:898/toolboxes/smc.tbx#This Computer (crusher)/System Configuration/Users/User Accounts/

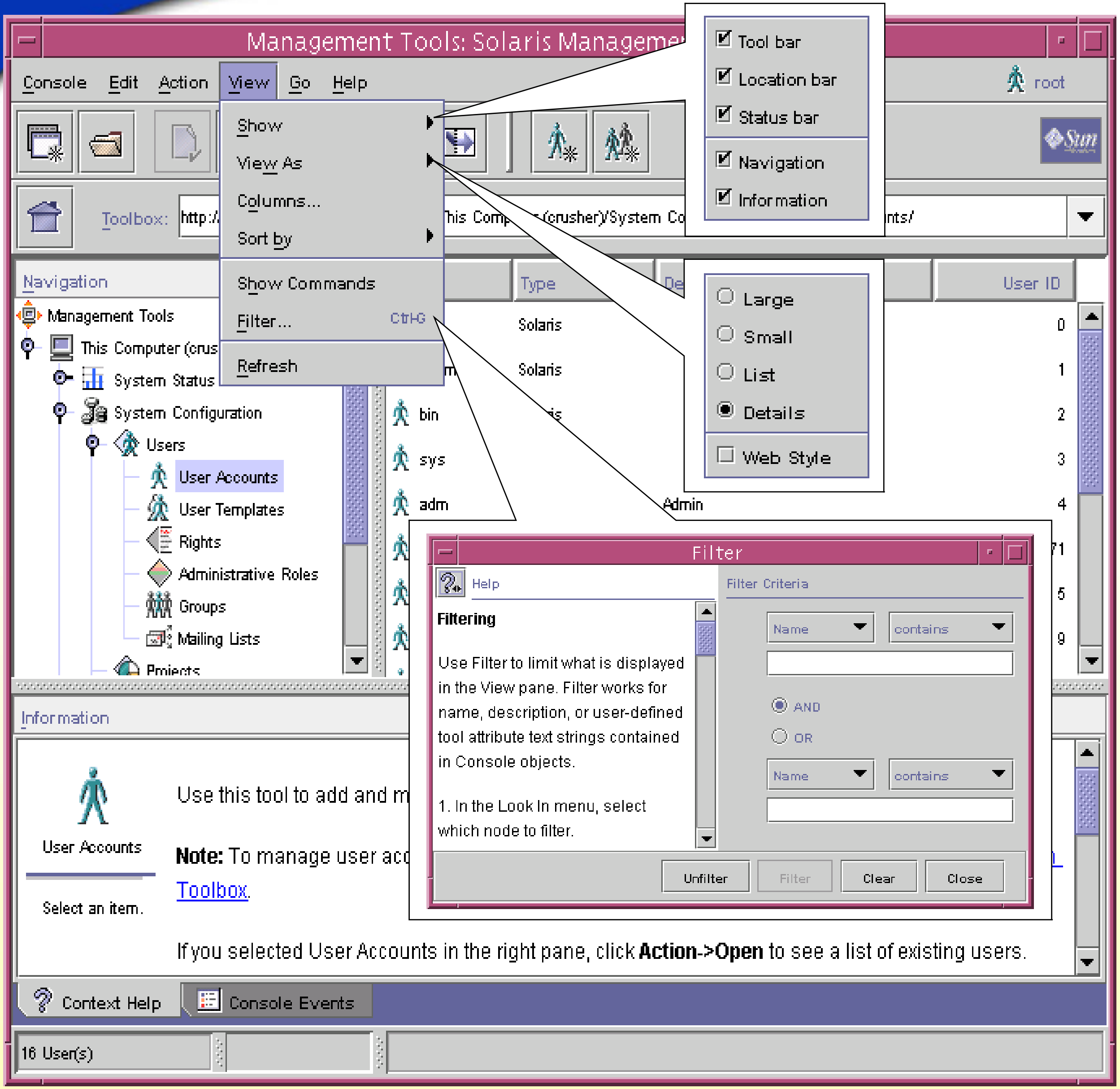
Name	Type	Description	User ID
root	Solaris	Super-User	0
daemon	Solaris		1
bin	Solaris		2
sys	Solaris		3
adm	Solaris	Admin	4
lp	Solaris	Line Printer Admin	71
uucp	Solaris	uucp Admin	5
nuucp	Solaris	uucp Admin	9

Use this tool to add and manage user accounts.

Note: To ma service domain, see To Create a Name Service Domain Toolbox.

If you selected U r Accounts in the right pane, click **Action->Open** to see a list of existing users.

SMC – Main Window Overview Cont.



Filtering

Use Filter to limit what is displayed in the View pane. Filter works for name, description, or user-defined tool attribute text strings contained in Console objects.

1. In the Look In menu, select which node to filter.

Use this tool to add and m

Note: To manage user acc

Toolbox.

If you selected User Accounts in the right pane, click **Action->Open** to see a list of existing users.

- **SMC allows a user to**
  - select which SMC display components will be shown
  - select the format of the view pane
  - sort the view pane by columns
  - use a filter to determine which object will be displayed in the view pane

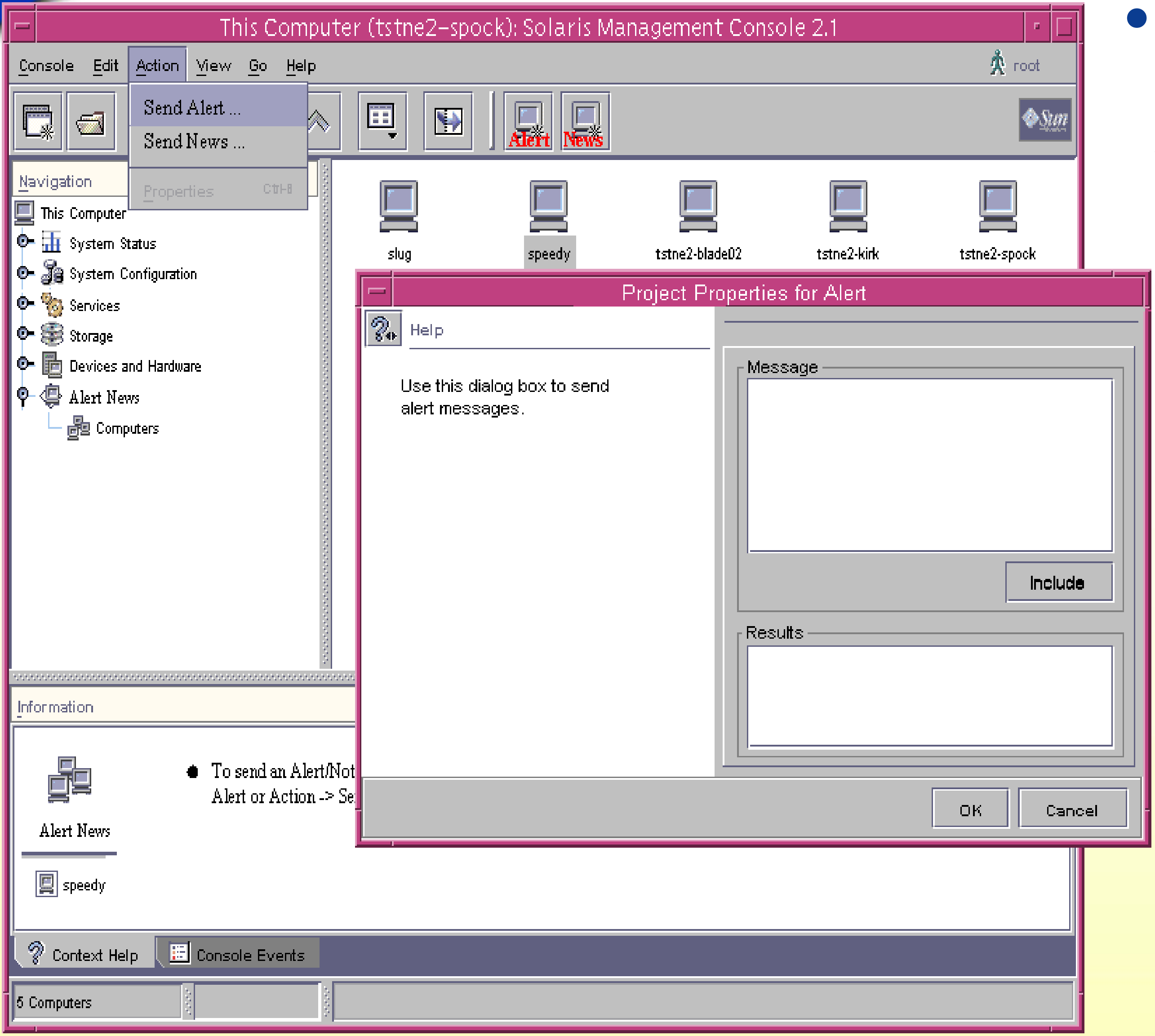
SMC – Application Requirements

- **Each JEDI application ported to the SMC framework will**
  - Have a tool descriptor file that contains
    - A large icon
    - A small icon
    - A description
    - A help file
  - Update the center pane of the Status Bar (Console Activity Indicator)
  - Update the Status Bar (Message Area)
  - Log to the SMC Event Log
  - Add appropriate information to the Menu Bar and Icon Bar
  - Support RBAC

SMC – Transitioned Applications

- **JEDI TFM applications that will be transitioned to SMC include**
  - Alert News
  - Archive Utility
  - Assign Credentials (Host/User)
  - Assign Passwords
  - Boot Utility
  - Change File Information
  - Disk Space
  - Network Status
  - Session Maintenance
  - User Session Maintenance
  - User Account Information

SMC – Alert News

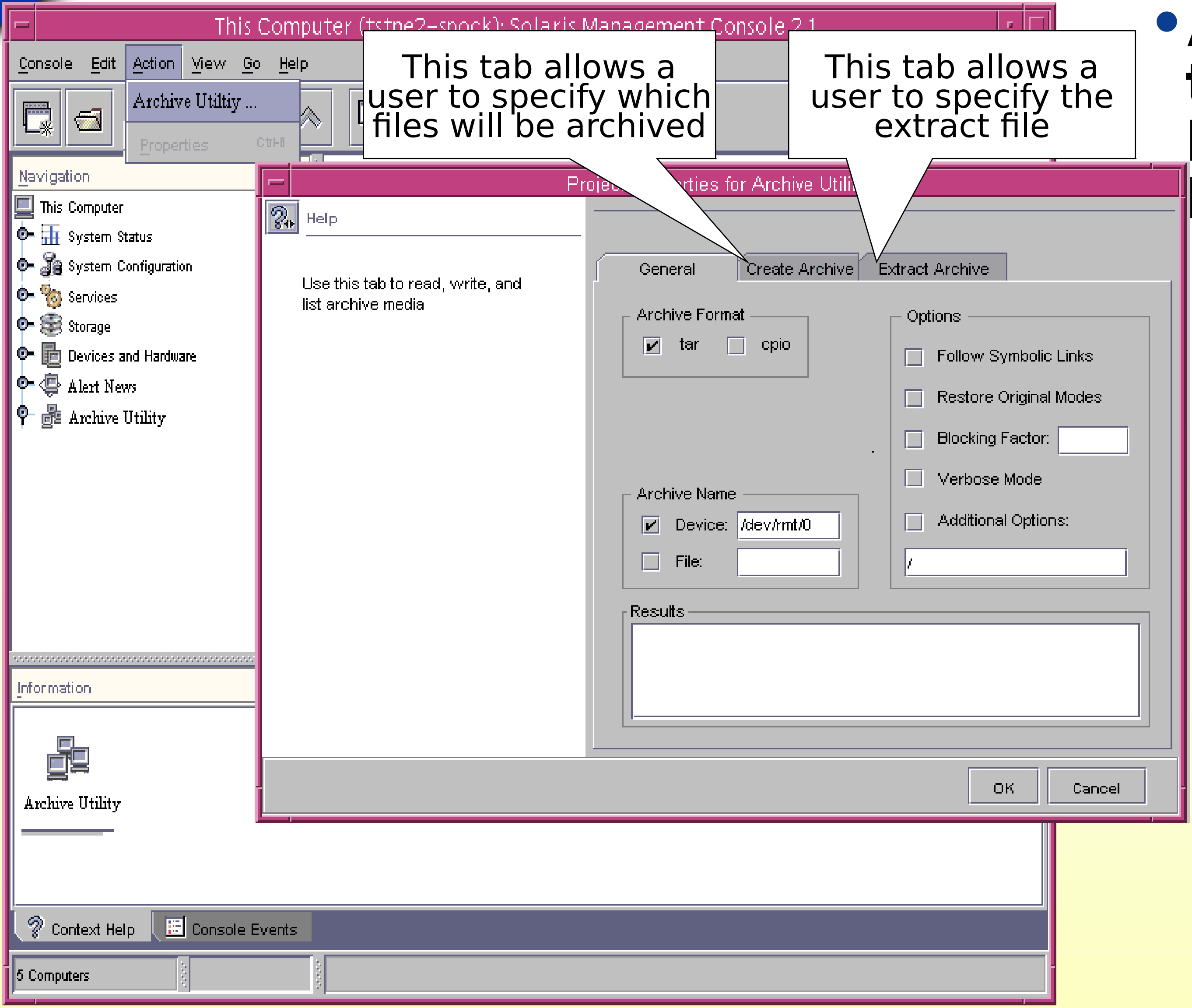


Use this dialog box to send alert messages.

- To send an Alert/Not
Alert or Action -> Se

- **Provides the ability to send Alerts/Sign on News to a workstation(s)**
  - Invoked from new menu/icon options
  - Same interface for both the Alert and Sign on News dialog
  - Workstations are selected from a list of icons displayed in the view pane

SMC – Archive Utility



This tab allows a user to specify which files will be archived

This tab allows a user to specify the extract file

Use this tab to read, write, and list archive media

Archive Format
☑ tar □ cpio

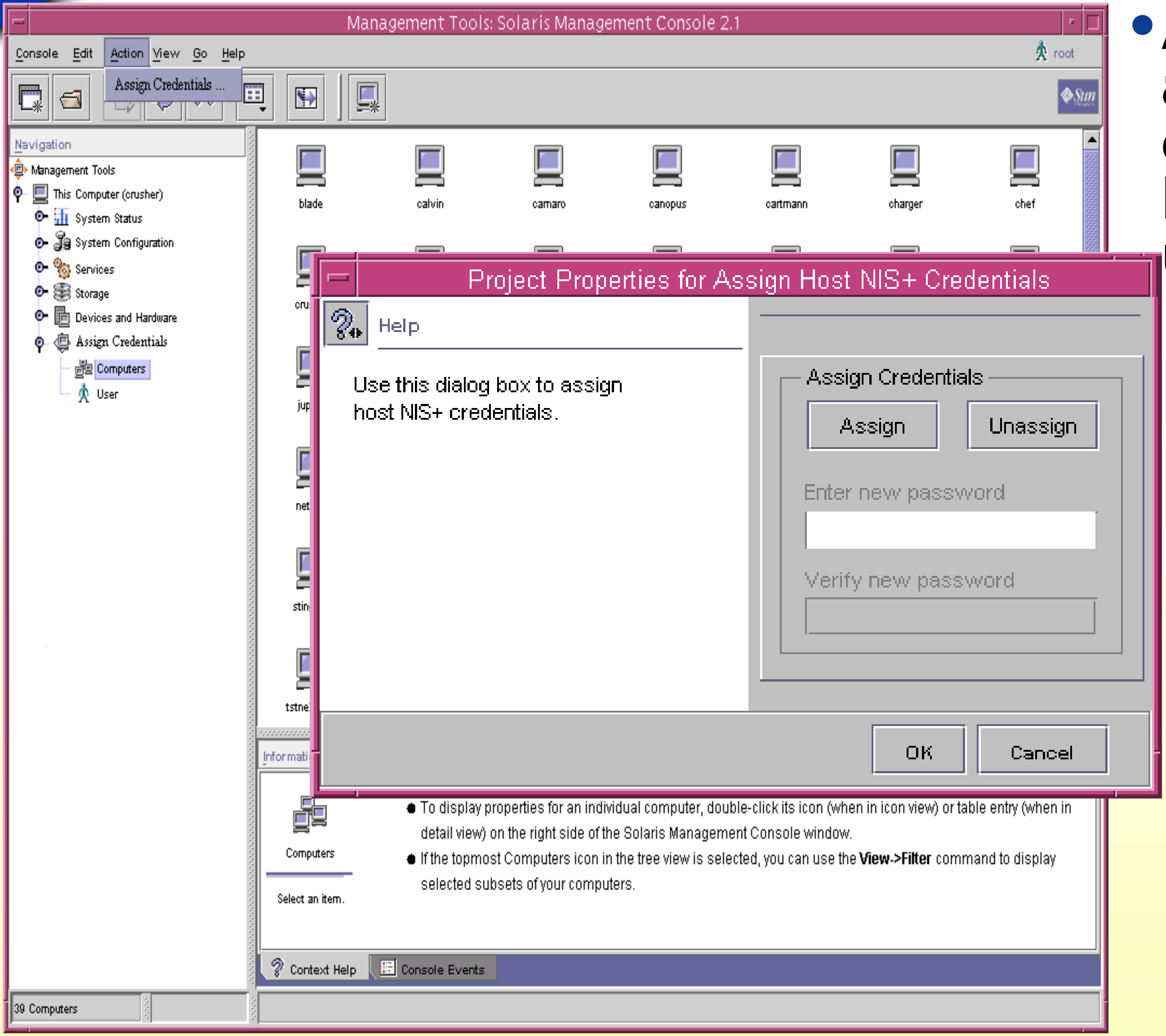
Archive Name
☑ Device: /dev/rmt/0
□ File:

Options
□ Follow Symbolic Links
□ Restore Original Modes
□ Blocking Factor:
□ Verbose Mode
□ Additional Options:
/

Results

- **Allows a user to Archive Files / Directories**
  - Invoked from the menu/icon bar
  - Follows the JEDI V1.3 functionality

SMC – Assign Credentials

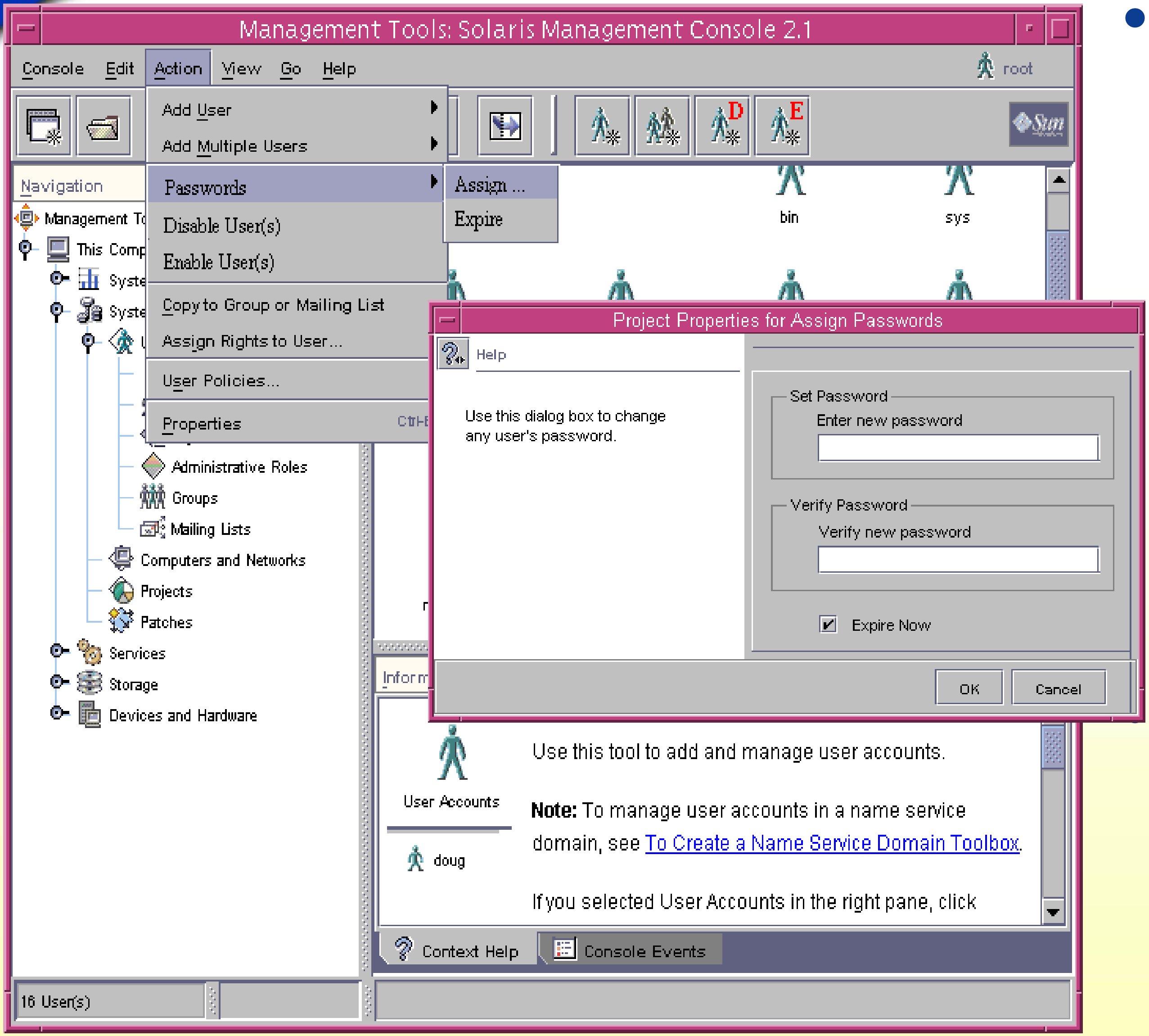


Use this dialog box to assign host NIS+ credentials.

- To display properties for an individual computer, double-click its icon (when in icon view) or table entry (when in detail view) on the right side of the Solaris Management Console window.
- If the topmost Computers icon in the tree view is selected, you can use the **View->Filter** command to display selected subsets of your computers.

- **Allows a user to assign credentials for both host and users**
  - Similar interface for both hosts and users
  - Uses the View->Filter option to select
    - All Hosts
    - Hosts with credentials
    - Host without credentials

SMC – Assign Passwords



Use this dialog box to change any user's password.

Set Password
Enter new password

Verify Password
Verify new password

☑ Expire Now

Use this tool to add and manage user accounts.

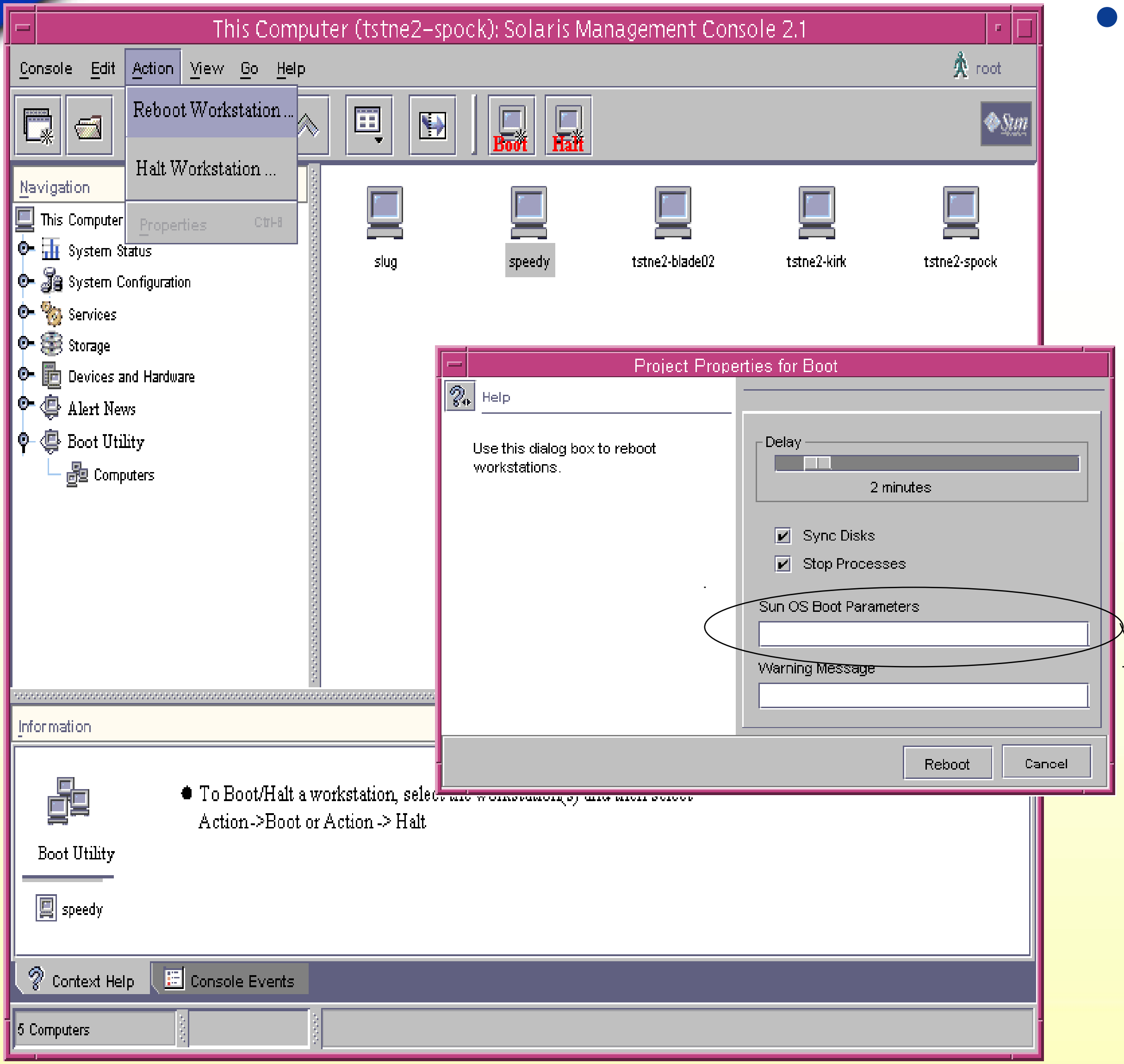
Note: To manage user accounts in a name service domain, see To Create a Name Service Domain Toolbox.

If you selected User Accounts in the right pane, click

- **Allows an administrator to Assign/Expire a password(s)**
  - Invoked from new menu/icon options
  - User(s) are selected from a list of icons displayed in the view pane

Assigned Passwords will be grouped under User Account Maintenance

SMC – Boot Utility



Use this dialog box to reboot workstations.

Delay: 2 minutes

☑ Sync Disks

☑ Stop Processes

Sun OS Boot Parameters:

Warning Message:

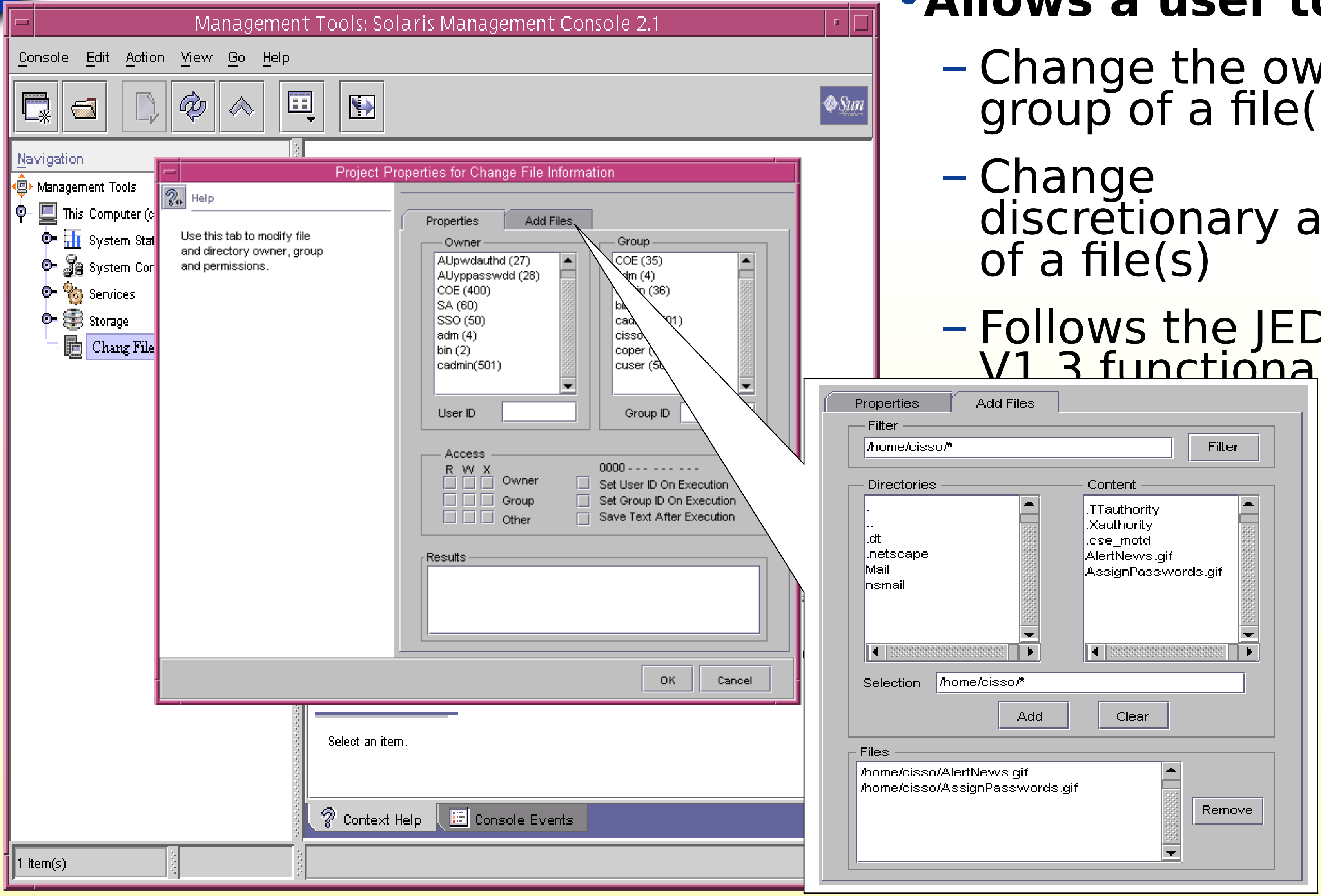
- To Boot/Halt a workstation, select the workstation(s) and then select Action->Boot or Action -> Halt

- **Allows an administrator to Reboot/Halt a workstation(s)**
  - Invoked from new menu/icon options
  - Host(s) are selected from a list of icons displayed in the view pane
  - Common interface for both Halt and Reboot

Note: The "OS Boot Parameters" will only be displayed when a workstation is Rebooted

SMC – Change File Information

- **Allows a user to**
  - Change the owner / group of a file(s)
  - Change discretionary access of a file(s)
  - Follows the JEDI V1.3 functionality



Management Tools: Solaris Management Console 2.1

Project Properties for Change File Information

Use this tab to modify file and directory owner, group and permissions.

Owner: AUpwdauthd (27), AUyppasswdd (28), COE (400), SA (60), SSO (50), adm (4), bin (2), cadmin(501)

Group: COE (35), adm (4), [illegible] (36), bi[illegible], cad[illegible] [illegible]01), cisso, coper (, cuser (50

User ID:

Group ID:

Access

	R	W	X
Owner	□	□	□
Group	□	□	□
Other	□	□	□

0000 - - - - - - - - -

□ Set User ID On Execution
□ Set Group ID On Execution
□ Save Text After Execution

Results

Filter: /home/cisso/*

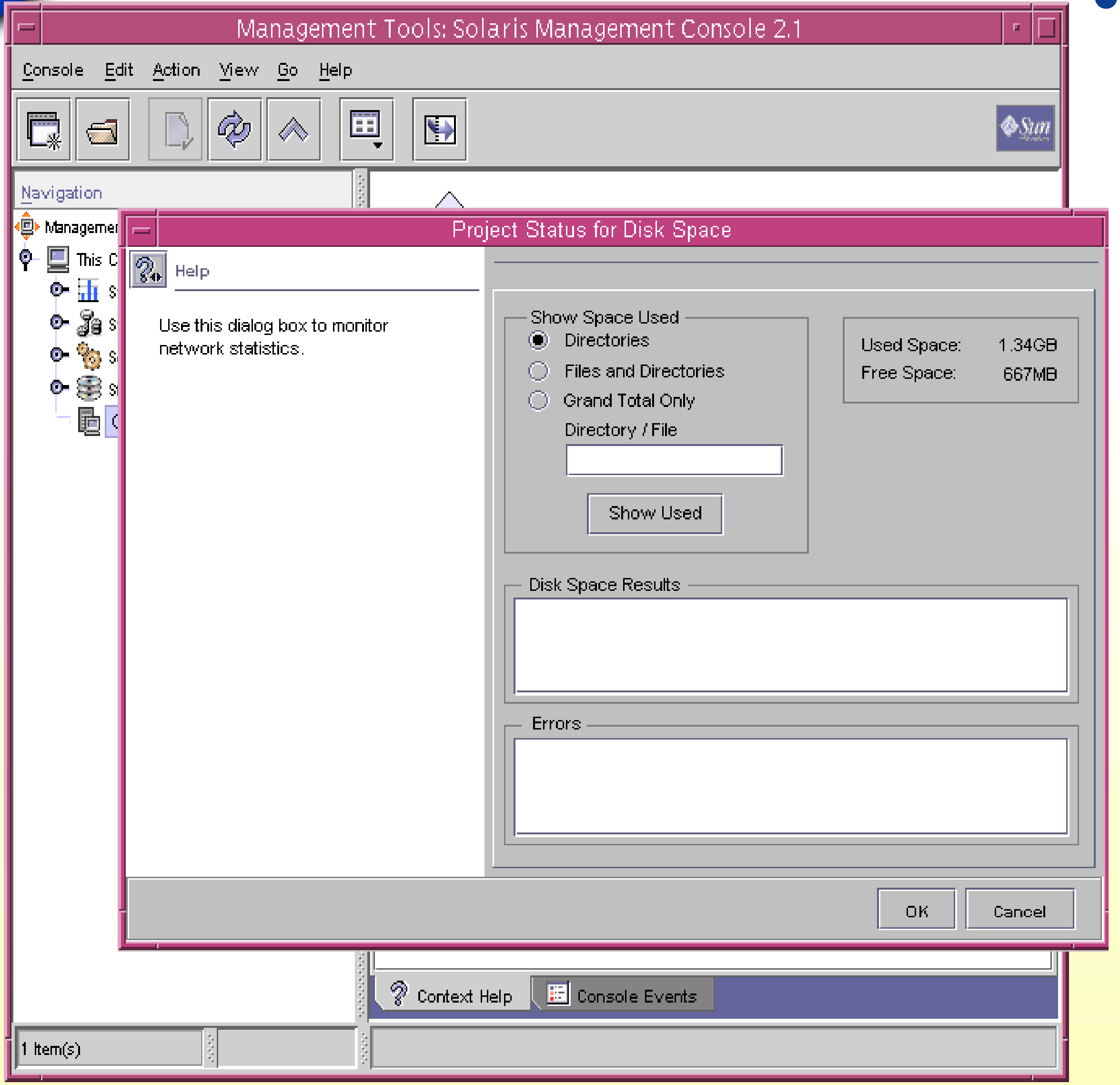
Directories: ., .., .dt, .netscape, Mail, nsmail

Content: .TTauthority, .Xauthority, .cse_motd, AlertNews.gif, AssignPasswords.gif

Selection: /home/cisso/*

Files:
/home/cisso/AlertNews.gif
/home/cisso/AssignPasswords.gif

SMC – Disk Space



Use this dialog box to monitor network statistics.

Show Space Used

● Directories
○ Files and Directories
○ Grand Total Only

Directory / File

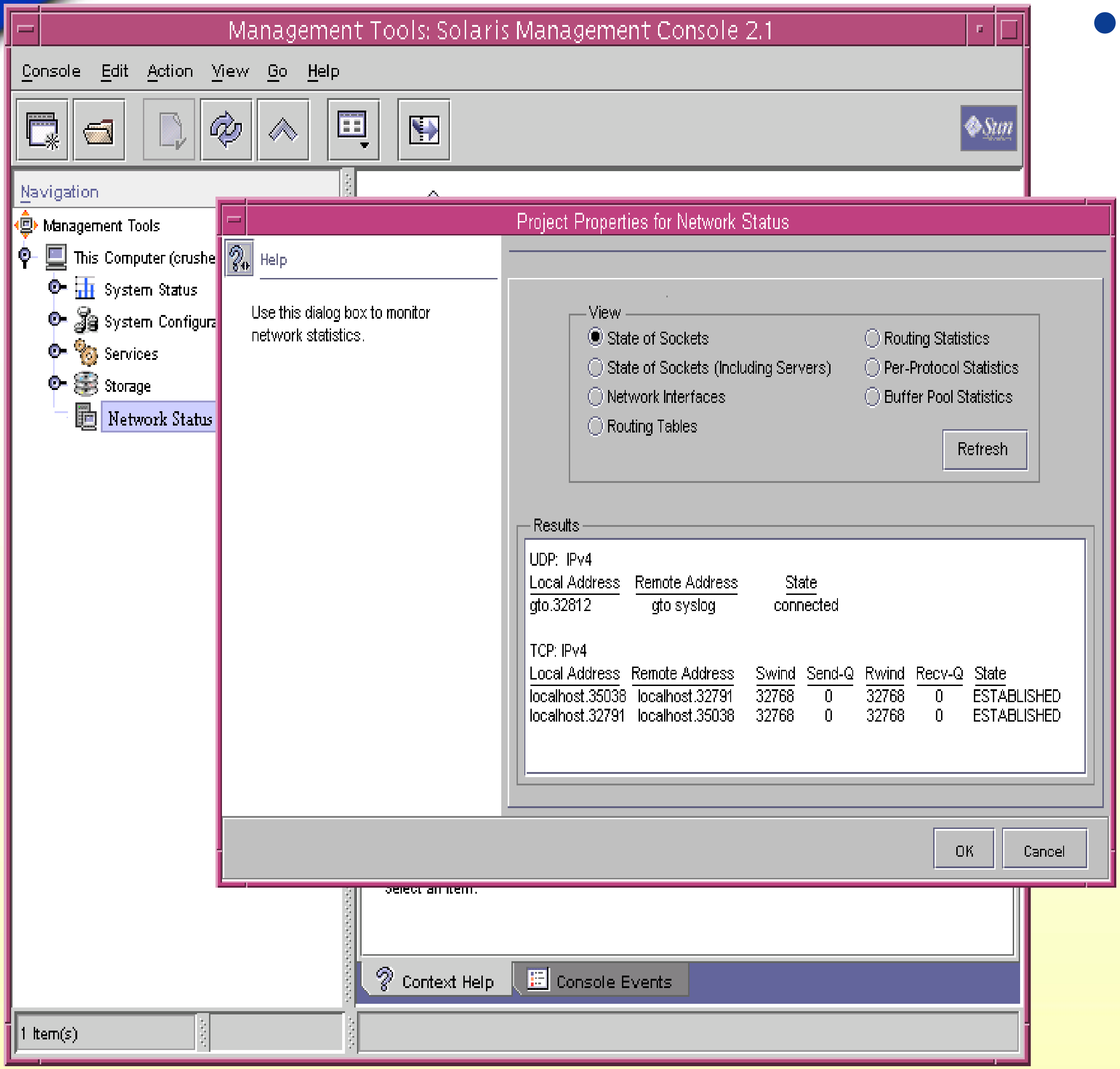
Used Space: 1.34GB
Free Space: 667MB

Disk Space Results

Errors

- **Allows a user to**
  - Use the SMC navigation/view pane to drill down to a workstation
  - Use the property sheet for the specified workstation
    - Space Used
    - Free Space

SMC – Network Status



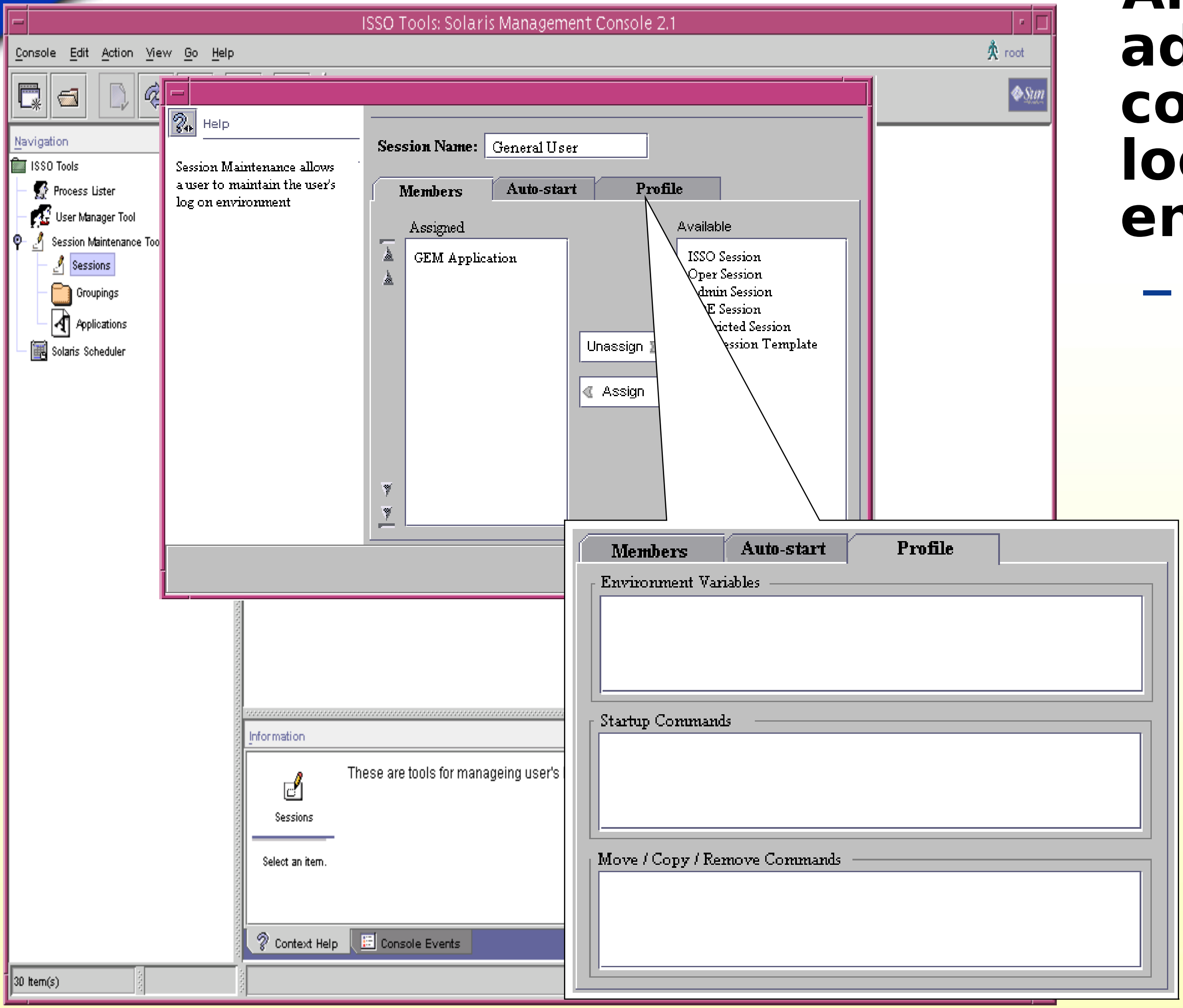
Use this dialog box to monitor network statistics.

View: ● State of Sockets

```
UDP: IPv4
Local Address   Remote Address     State
gto.32812        gto syslog       connected

TCP: IPv4
Local Address    Remote Address   Swind  Send-Q  Rwind  Recv-Q  State
localhost.35038  localhost.32791  32768    0     32768    0     ESTABLISHED
localhost.32791  localhost.35038  32768    0     32768    0     ESTABLISHED
```

- **Allows a user to**
  - Show network statistics
  - Follows the JEDI V1.3 functionality

SMC – Session Maintenance



Session Maintenance allows a user to maintain the user's log on environment

Session Name: General User

Assigned: GEM Application

Available: ISSO Session, Oper Session, dmin Session, E Session, icted Session, ssion Template

These are tools for manageing user's

Sessions

Select an item.

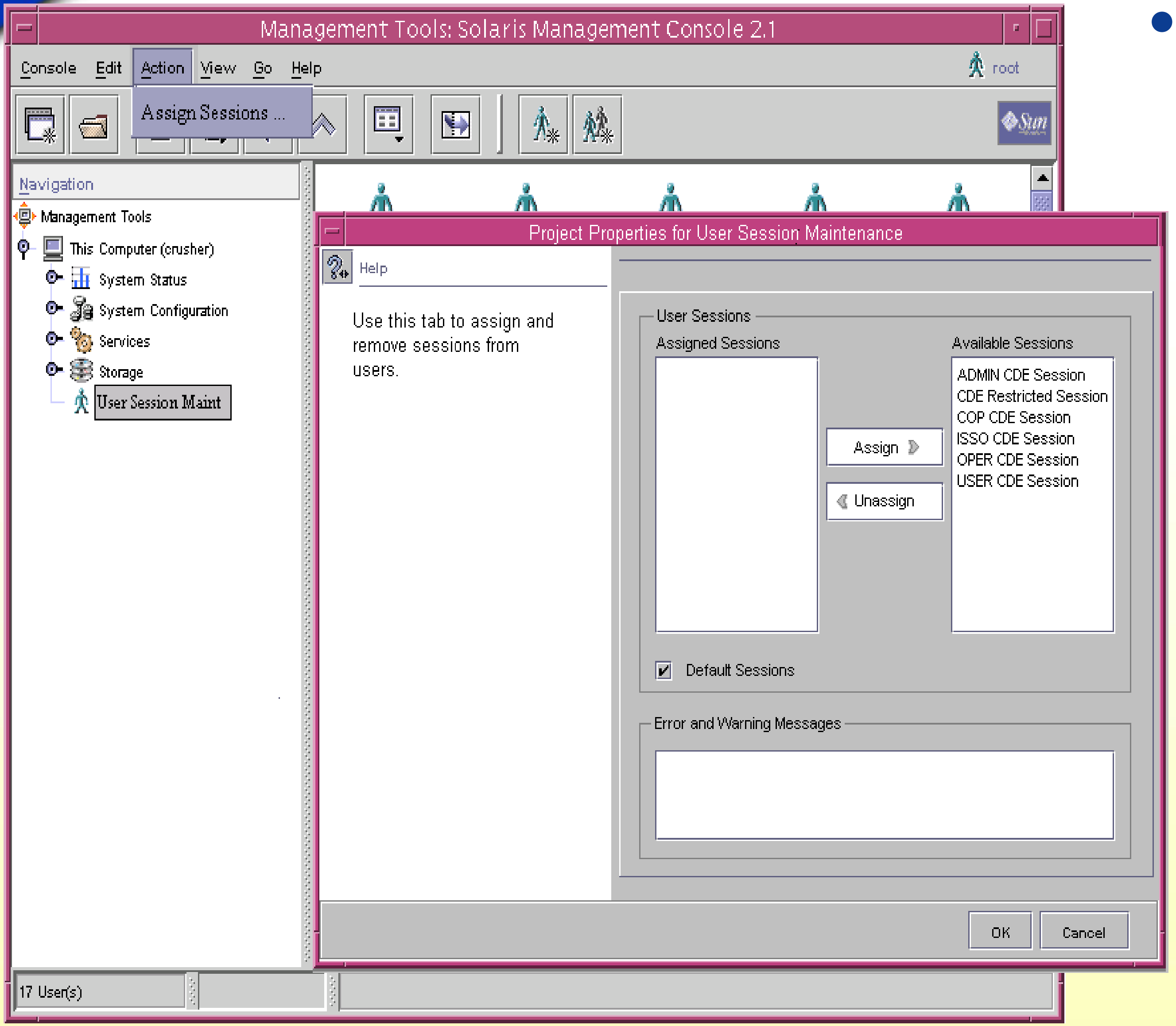
Environment Variables

Startup Commands

Move / Copy / Remove Commands

- **Allows an administrator to control a user's log on environment**
  - Supports menu/ icon options to
    - Add
    - Delete
    - Modify

SMC – User Session Maintenance



Project Properties for User Session Maintenance

Use this tab to assign and remove sessions from users.

User Sessions

Assigned Sessions

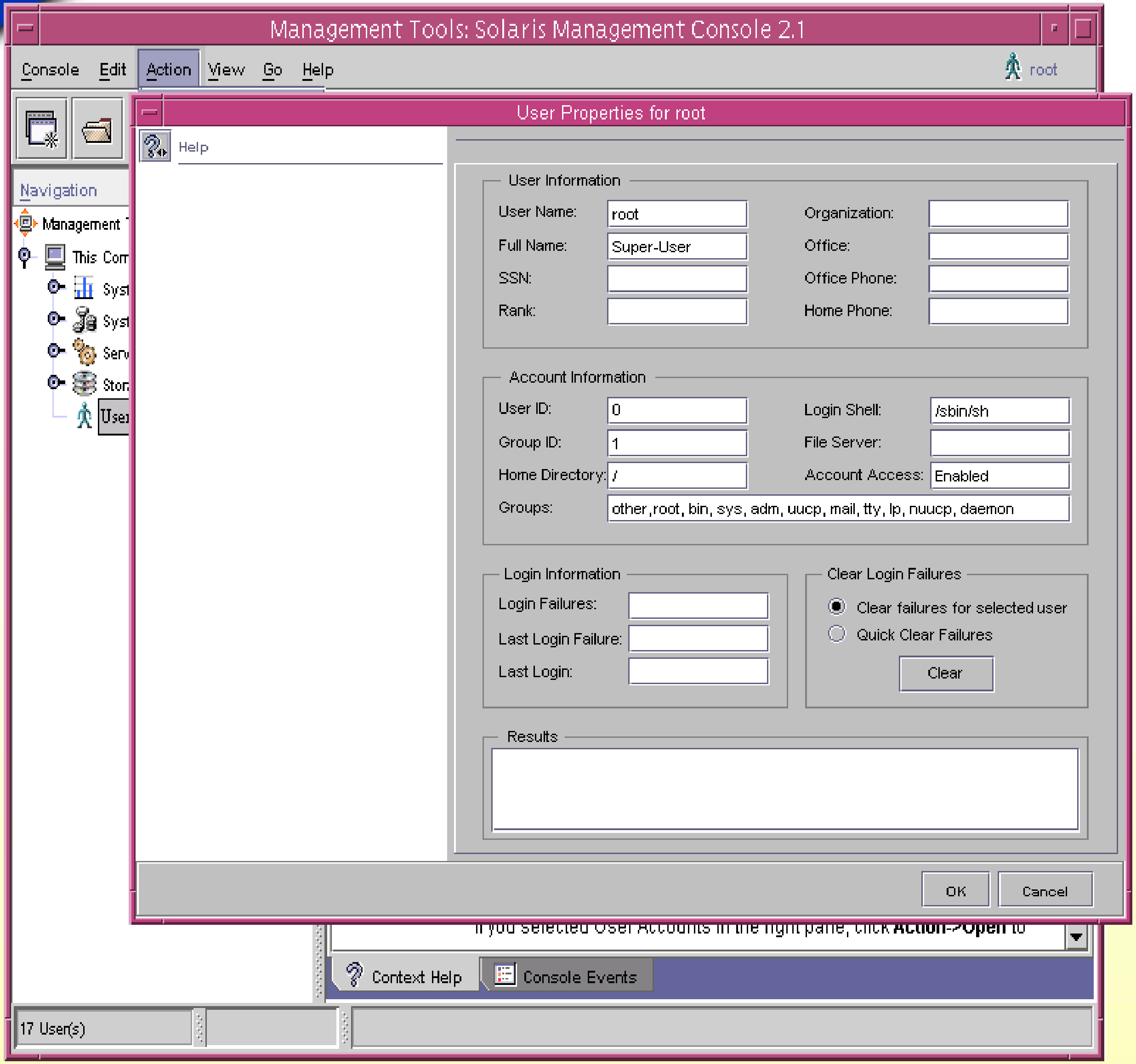
Available Sessions
ADMIN CDE Session
CDE Restricted Session
COP CDE Session
ISSO CDE Session
OPER CDE Session
USER CDE Session

☑ Default Sessions

Error and Warning Messages

- **Allows a user to assign Sessions to a user/list of users**
  - A list of users is displayed in the view pane
  - Multiple users may be selected

SMC – User Account Information



User Information

User Name:	root	Organization:	
Full Name:	Super-User	Office:	
SSN:		Office Phone:	
Rank:		Home Phone:	

Account Information

User ID:	0	Login Shell:	/sbin/sh
Group ID:	1	File Server:	
Home Directory:	/	Account Access:	Enabled
Groups:	other,root, bin, sys, adm, uucp, mail, tty, lp, nuucp, daemon		

Login Information

Login Failures:	
Last Login Failure:	
Last Login:	

Clear Login Failures

● Clear failures for selected user

○ Quick Clear Failures

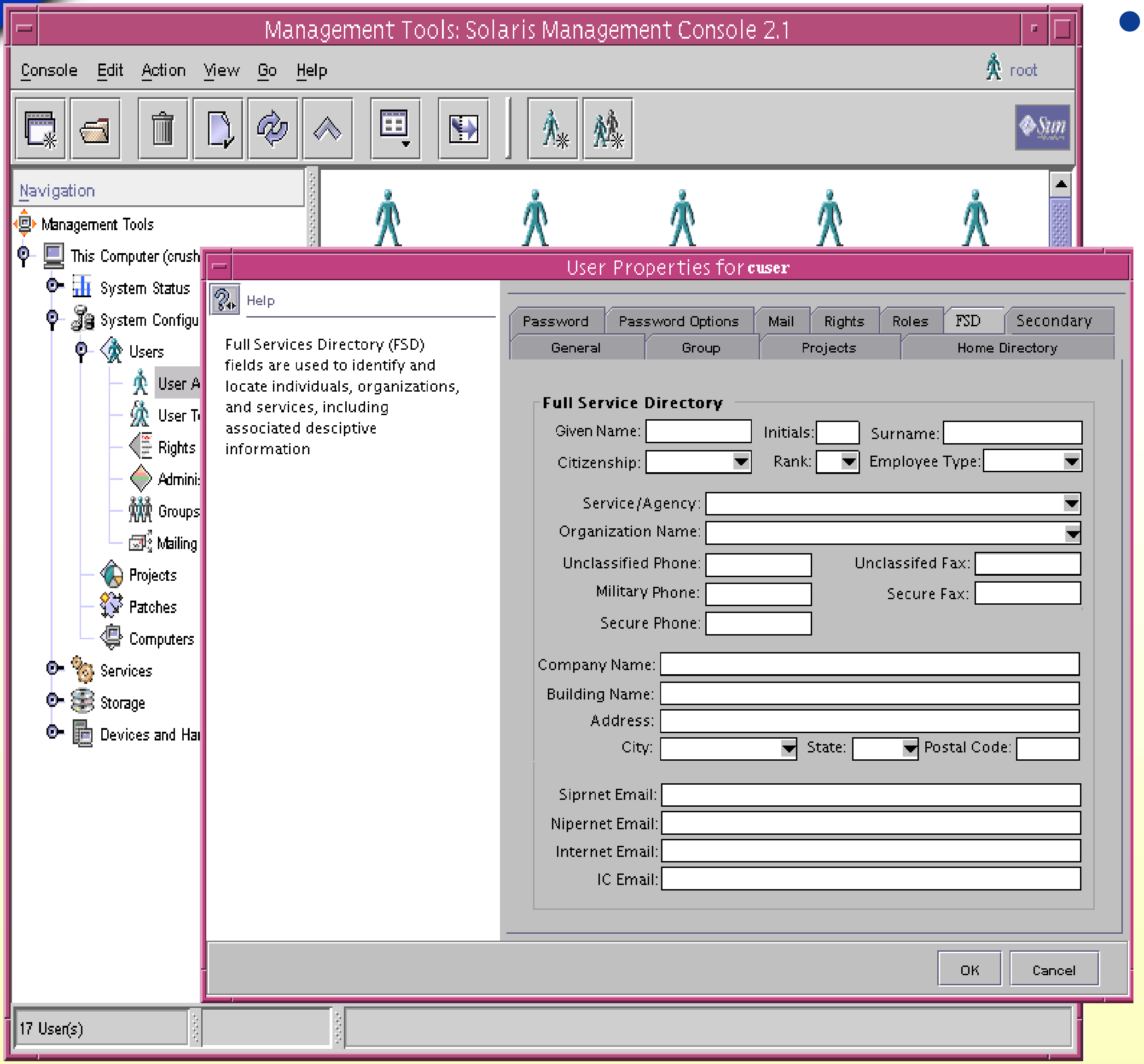
Results

- **Allows a user to view User Account Information**
  - Use the SMC navigation/view pane to drill down to a user
  - Use the property sheet to view information about the specified user
  - Use the SMC filter to limit the users displayed in the view pane

SMC – COTS Migration

- **The following Trusted JEDI applications have been replaced with SMC Applications**
  - User Maintenance
  - Process Management
  - Printer Maintenance
  - Printer Status
  - Group Maintenance (no modifications made)
  - Host Maintenance (no modifications made)
- **Additional SMC Applications**
  - Dynamic Host Configuration Protocol

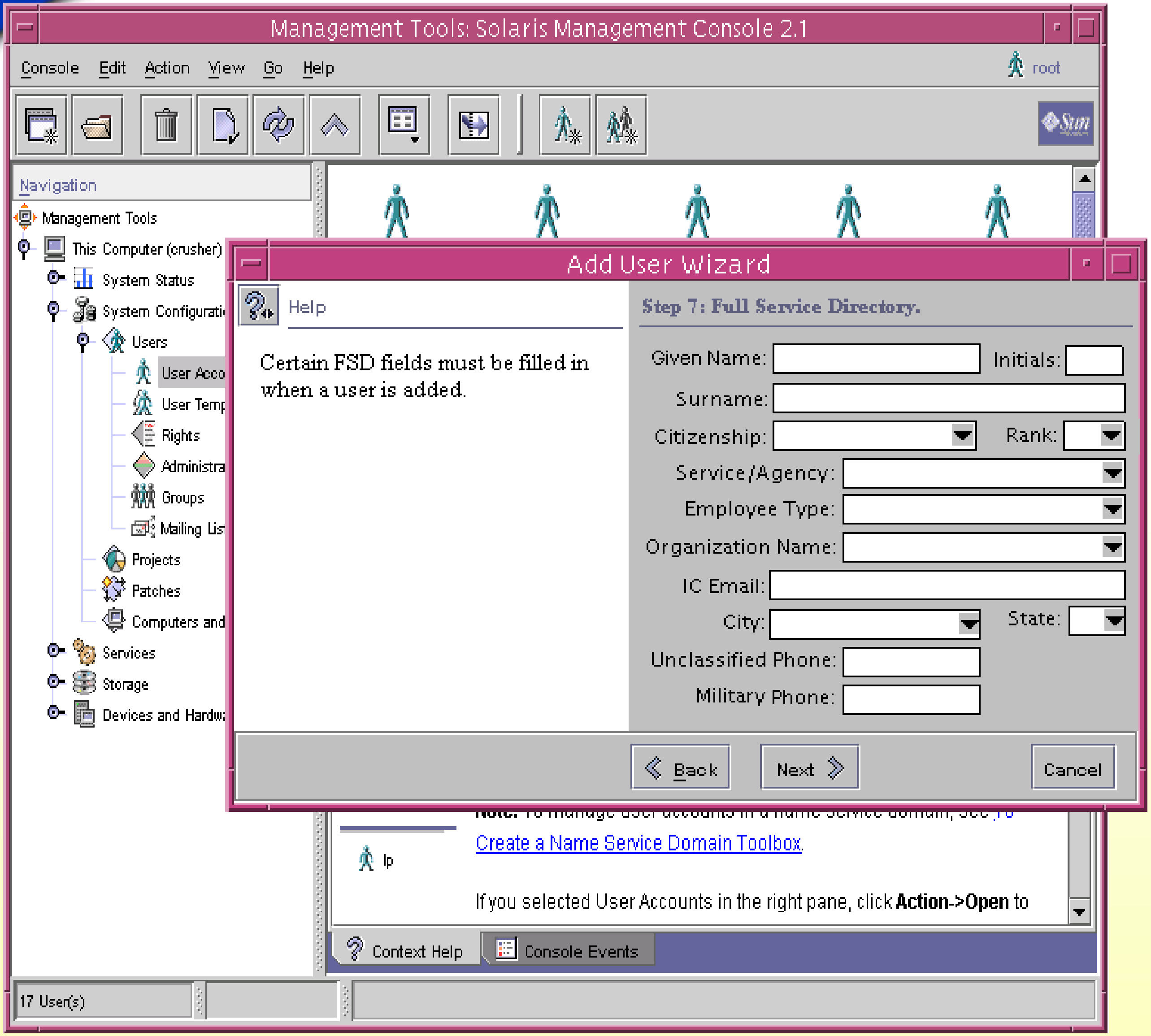
SMC – User Account Maintenance



Full Services Directory (FSD) fields are used to identify and locate individuals, organizations, and services, including associated desciptive information

- **The vendor-supplied User Maintenance property sheet will be extended to include**
  - Two new tabs for all Full Service Directory fields
  - Support for Add / Modify / Delete commands
  - Support drop down list for key Full Service Directory fields

SMC – User Account Maintenance Cont.



Step 7: Full Service Directory.

Certain FSD fields must be filled in when a user is added.

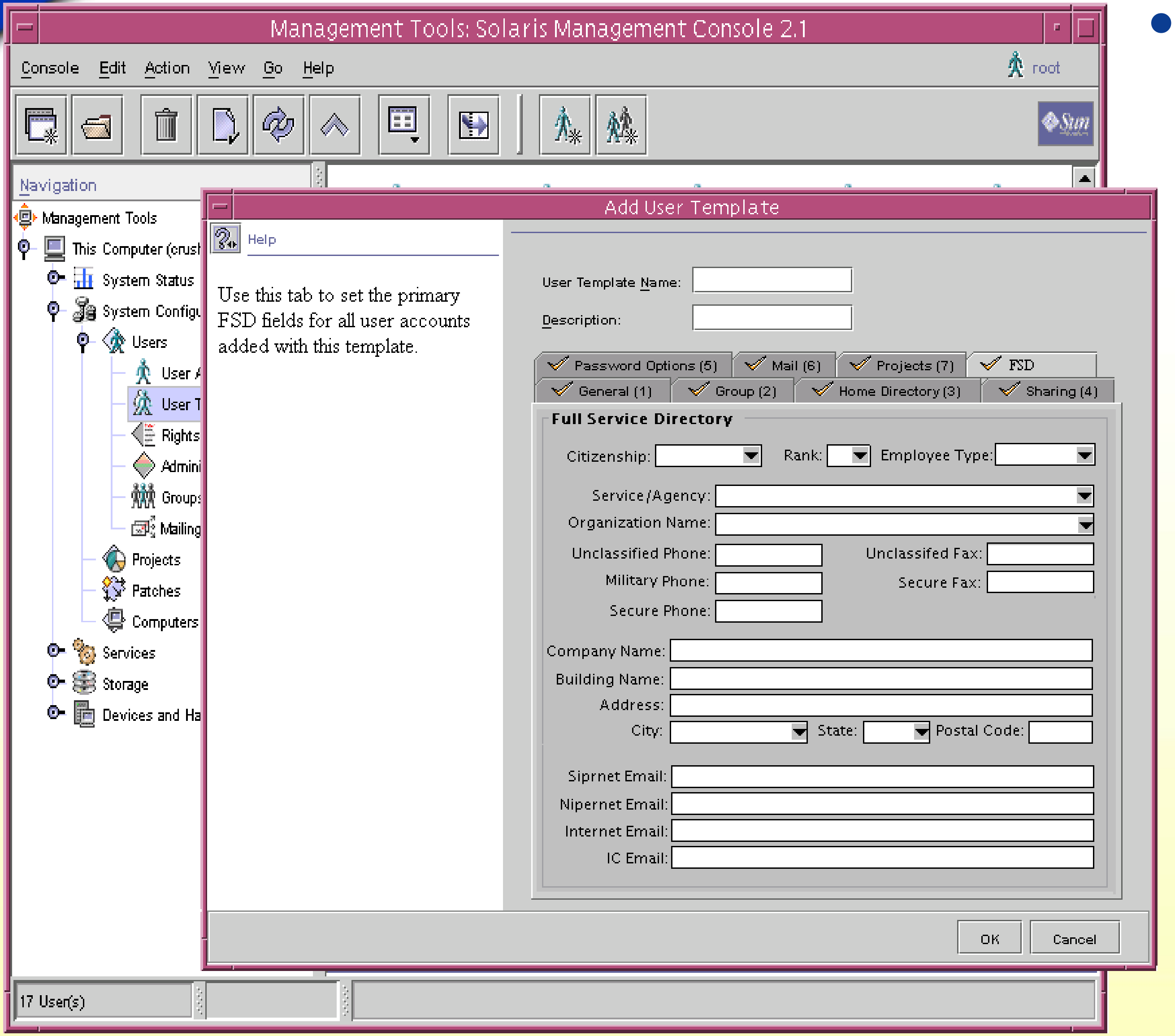
Note: To manage user accounts in a name service domain, see To

Create a Name Service Domain Toolbox

If you selected User Accounts in the right pane, click **Action->Open** to

- **The vendor-supplied User Maintenance Add User Wizard will be extended to include**
  - Pane for all mandatory Full Service Directory fields
- **Note: A configuration file must be created to store all FSD field information (including update information)**

SMC – User Account Maintenance Cont.

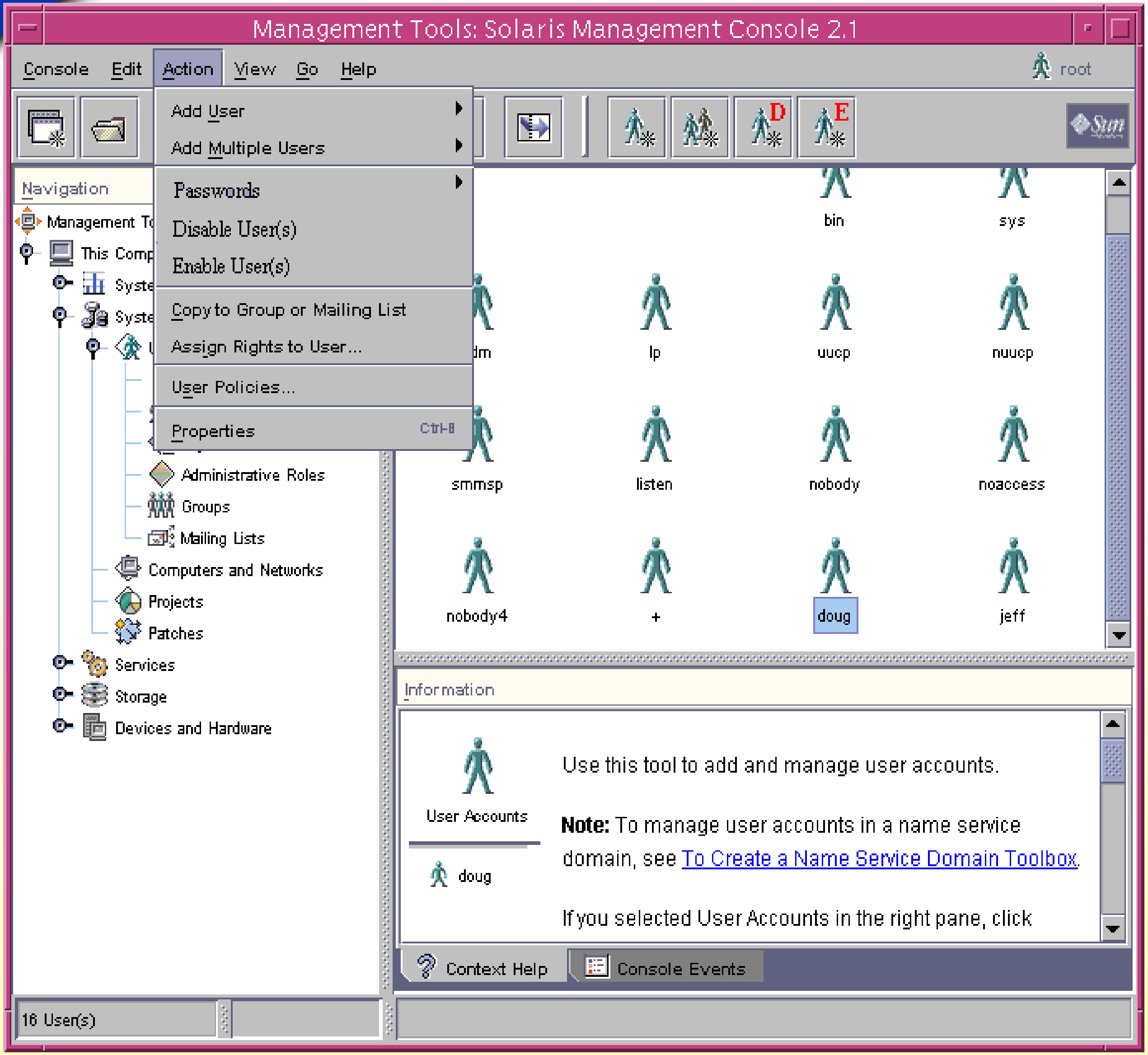


Use this tab to set the primary FSD fields for all user accounts added with this template.

- **The vendor-supplied User Maintenance User Templates will be extended to include**
  - Ability to set defaults for key Full Service Directory fields
  - Support drop down list for key Full Service Directory fields

NORTHROP GRUMMAN
Information Technology

SMC – User Account Maintenance Cont.



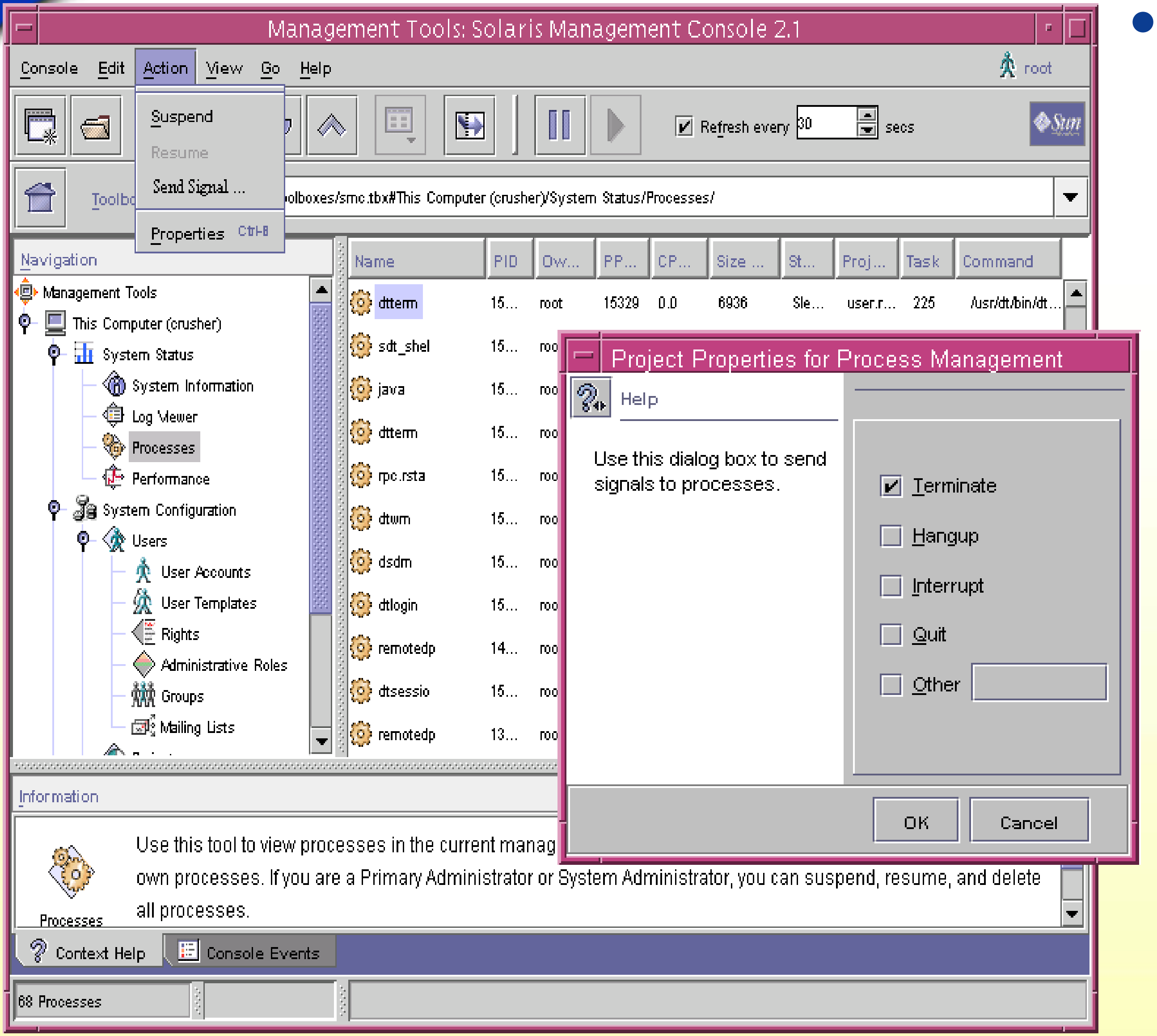
Use this tool to add and manage user accounts.

Note: To manage user accounts in a name service domain, see To Create a Name Service Domain Toolbox.

If you selected User Accounts in the right pane, click

- **The vendor-supplied User Maintenance Menu/Icon bar will be extended to include**
  - Menu/icon options for Enable Disable user accounts

SMC – Process Management



☑ Refresh every 30 secs

…olboxes/smc.tbx#This Computer (crusher)/System Status/Processes/

Name	PID	Ow...	PP...	CP...	Size ...	St...	Proj...	Task	Command
dtterm	15...	root	15329	0.0	6936	Sle...	user.r...	225	/usr/dt/bin/dt...
sdt_shel	15...	roo							
java	15...	roo							
dtterm	15...	roo							
rpc.rsta	15...	roo							
dtwm	15...	roo							
dsdm	15...	roo							
dtlogin	15...	roo							
remotedp	14...	roo							
dtsessio	15...	roo							
remotedp	13...	roo							

Use this dialog box to send signals to processes.

☑ Terminate

□ Hangup

□ Interrupt

□ Quit

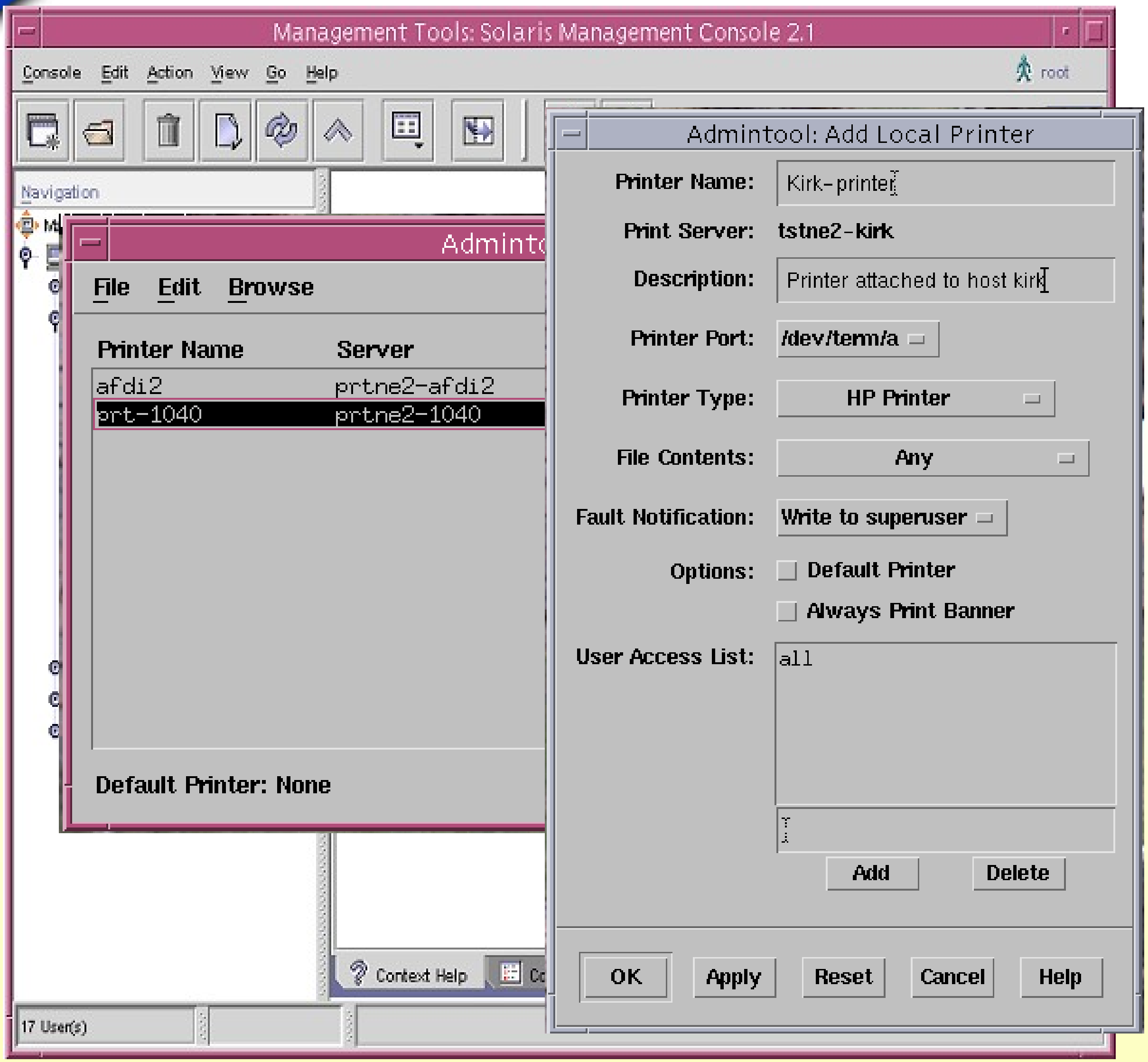
□ Other

Use this tool to view processes in the current manag own processes. If you are a Primary Administrator or System Administrator, you can suspend, resume, and delete all processes.

68 Processes

- **The vendor-supplied Process Management will be extended to**
  - allow a user to send additional signals to a process

SMC – Printer Maintenance


Management Tools: Solaris Management Console 2.1
Console Edit Action View Go Help
root
Navigation
Admintool
File Edit Browse
Admintool: Add Local Printer
Add
Delete
OK
Apply
Reset
Cancel
Help
Context Help
17 User(s)

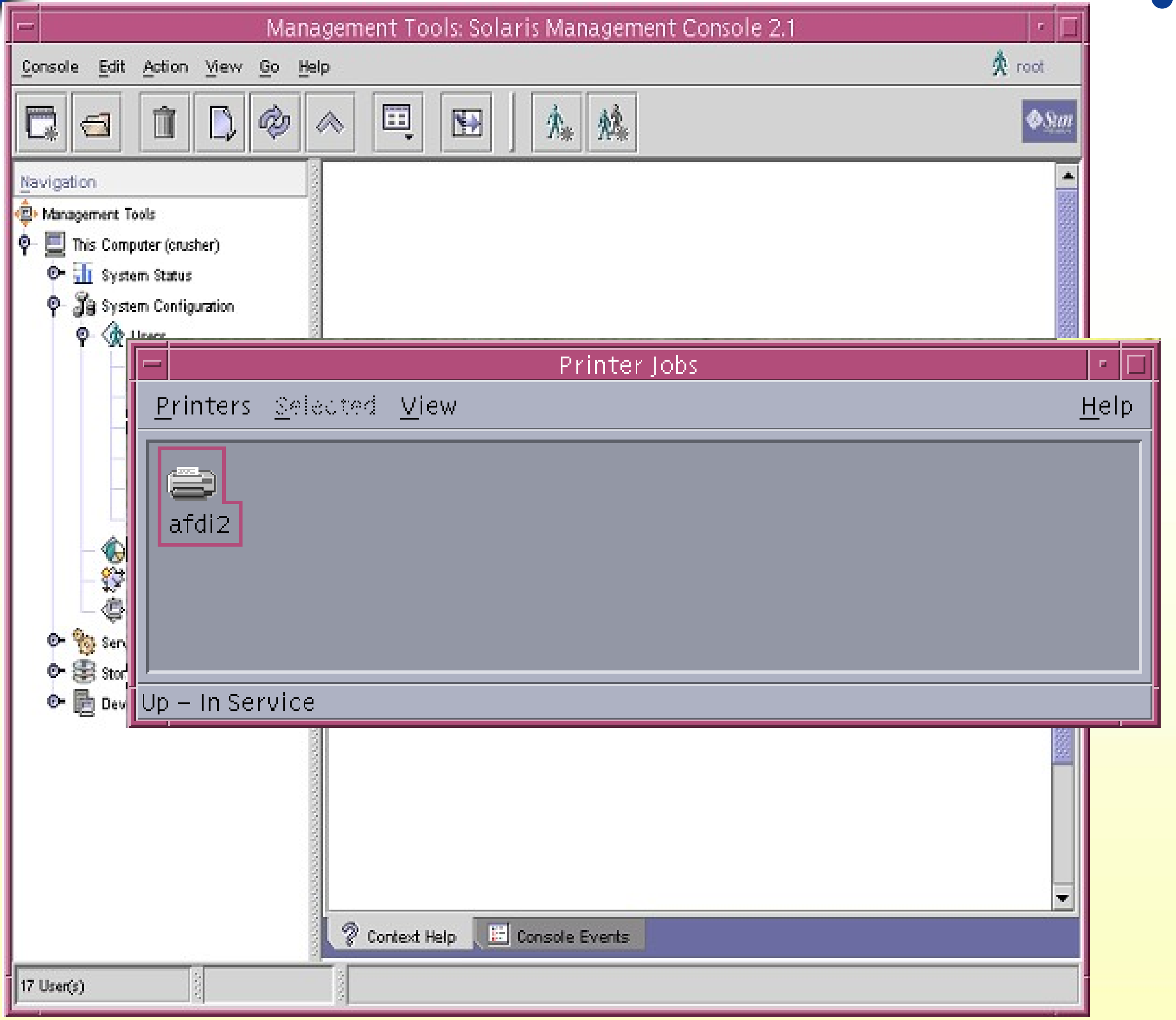
Printer Name	Server
afdi2	prtne2-afdi2
prt-1040	prtne2-1040

Default Printer: None

Printer Name: Kirk-printer
Print Server: tstne2-kirk
Description: Printer attached to host kirk
Printer Port: /dev/term/a
Printer Type: HP Printer
File Contents: Any
Fault Notification: Write to superuser
Options: □ Default Printer
□ Always Print Banner
User Access List: all

- **The vendor-supplied Admintool will be used to manage printers**
  - Launched from SMC

SMC – Privileged Printer Status



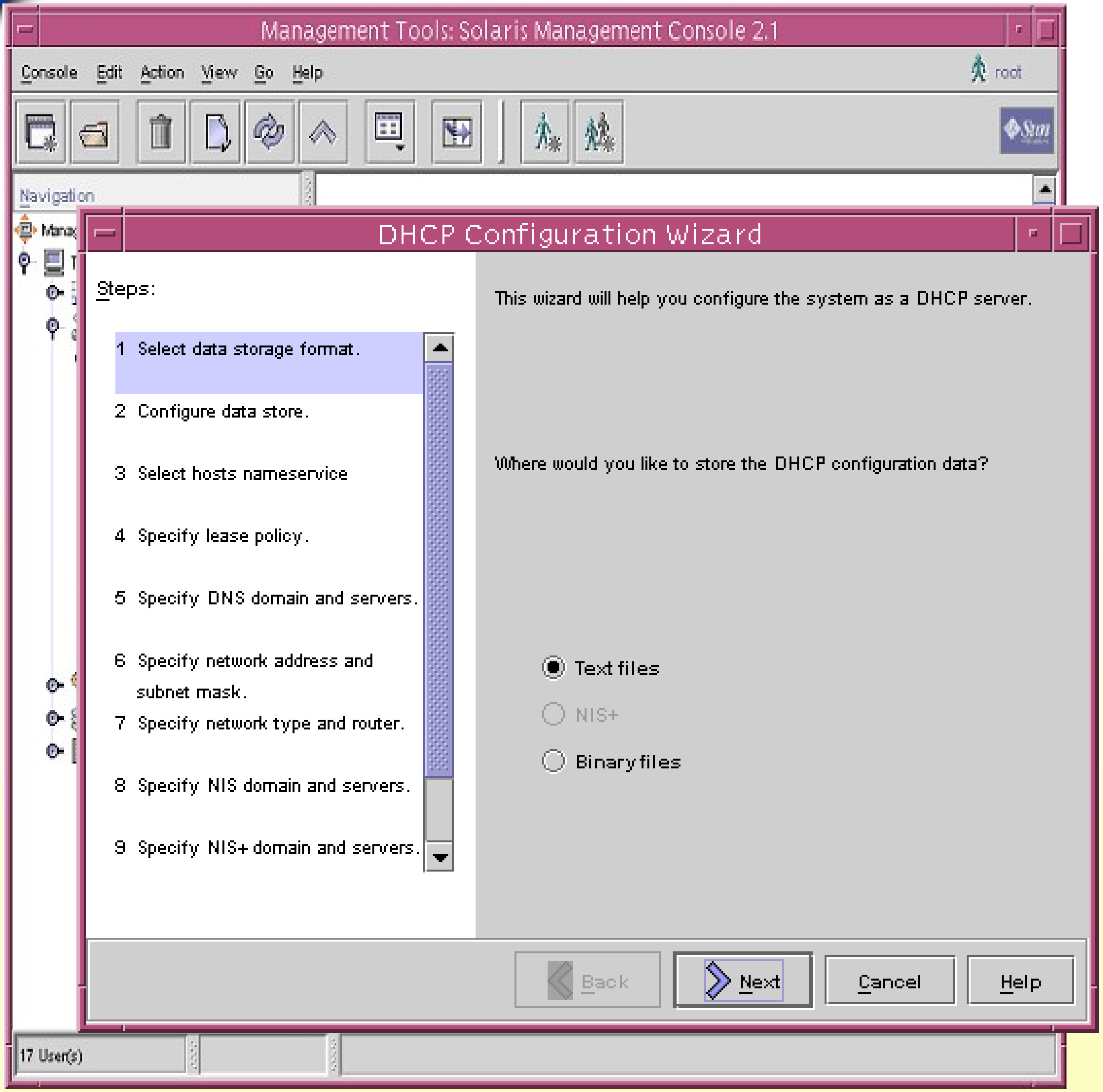
Up – In Service

- The vendor-supplied Printer Status utility will be used to manage print queues
  - Launched from the SMC

SMC – Dynamic Host Configuration Protocol

- **Dynamic Host Configuration Protocol (DHCP)**
  - Moves management of the IP addresses away from the client systems and onto centralized servers
  - Eliminates the need for clients to store static network information
  - Supports storing the entire configuration for the booting of diskless clients

SMC – Dynamic Host Configuration Protocol


Management Tools: Solaris Management Console 2.1
Console Edit Action View Go Help
root
Navigation
17 User(s)
DHCP Configuration Wizard
Back
Next
Cancel
Help

Steps:

1 Select data storage format.

2 Configure data store.

3 Select hosts nameservice

4 Specify lease policy.

5 Specify DNS domain and servers.

6 Specify network address and subnet mask.

7 Specify network type and router.

8 Specify NIS domain and servers.

9 Specify NIS+ domain and servers.

This wizard will help you configure the system as a DHCP server.

Where would you like to store the DHCP configuration data?

● Text files

○ NIS+

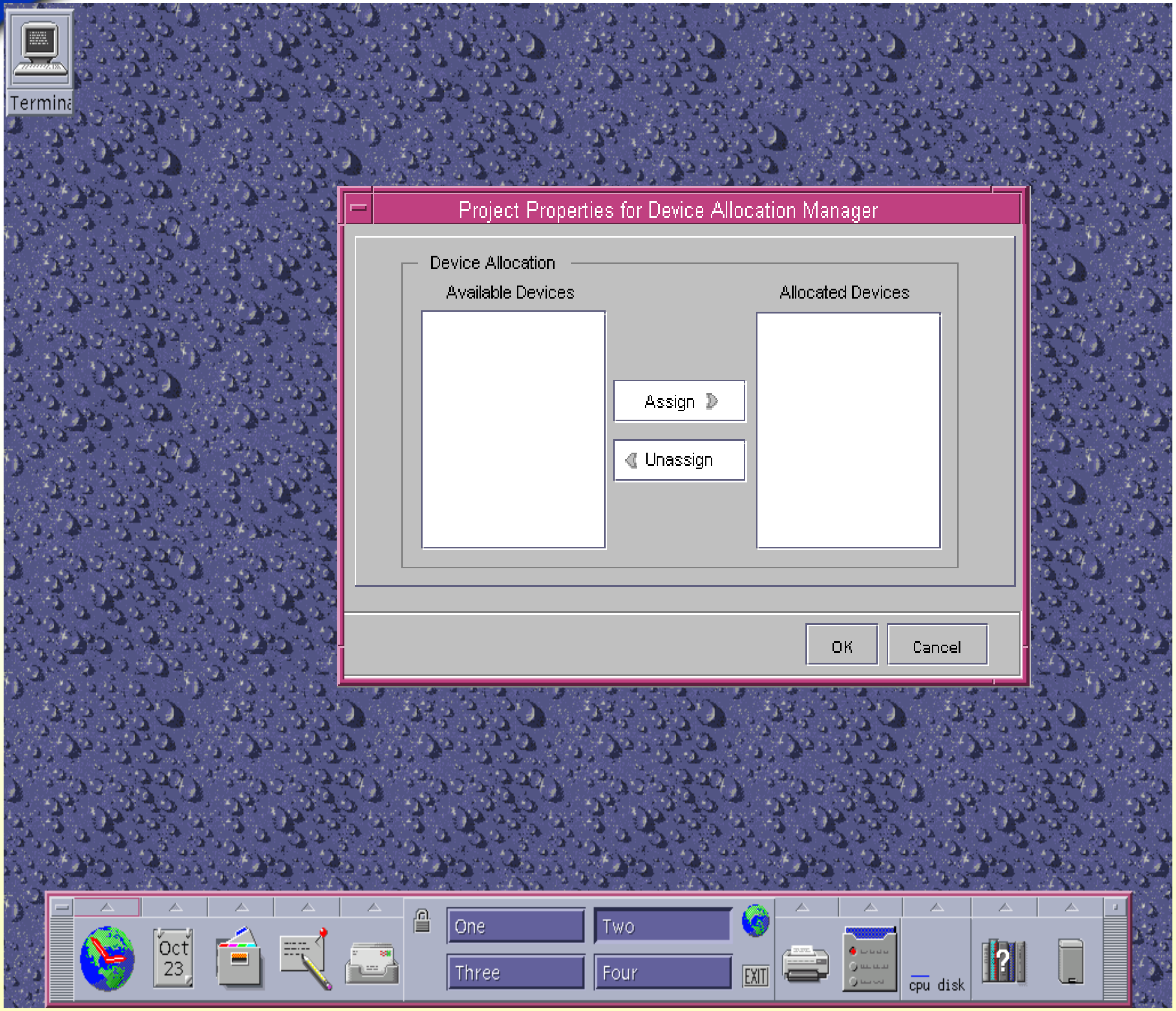
○ Binary files

- **Dynamic Host Configuration Protocol (DHCP)**
  - Launched from SMC
  - Minimal configuration will be documented in the ICG
- **May causes problems with DII/COE**
- **Adds another test configuration**

SMC – Legacy Applications

- **Some Trusted JEDI applications will be marked as legacy applications**
  - RBAC-enabled
  - Launched from the SMC
    - CLASS
    - RDIST (May move to SMC port)
  - Launched as a user application (Not an SMC application)
    - Ping
    - Allocate/Deallocate

SMC – Allocate/Deallocate



- **Allows a user to allocate / deallocate devices**
  - Graphical User Interface
  - Modified to support RBAC authorization checks
  - Launched from the background menu
  - Mirrors the Trusted Solaris implementation

SMC – Deprecated Applications

- **The following Trusted JEDI applications will be removed from the baseline**
  - Privilege Maintenance
  - General Tools
  - Shell Tool
  - SPI Tool
  - Protocol Maintenance

Roadmap

- **Solaris 9 Public Design Review**
  - JEDI 2.0 Requirements
  - Support for Solaris 9
  - Transition JEDI Tools to Role Based Access Control
  - ➡ Transition JEDI Tools to Solaris Management Console
  - Removing Dependency on JEDI Maps
  - Secure Shell
  - JASS Interface
  - Pluggable Authentication Modules
  - Flash Archive Support
  - Optional SASF for Solaris 9
  - Integration of ISS into JEDI 2.0 Baseline
  - Additional Recommendations

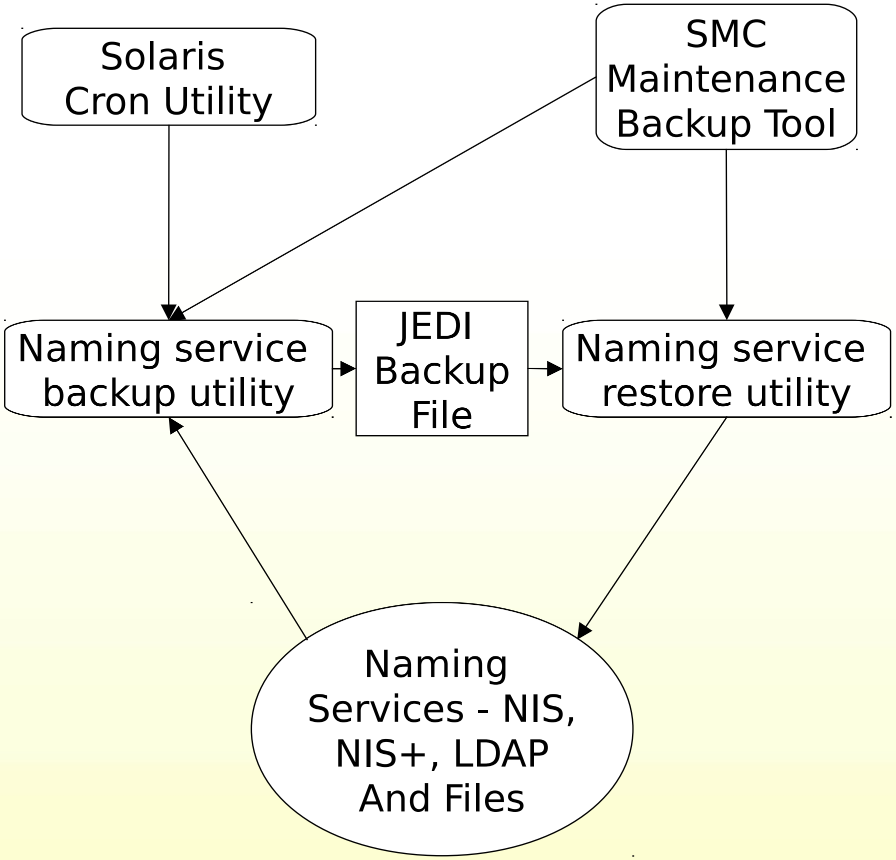
Roadmap – Maps Removal

- **Removing Dependency on JEDI Maps**
  - Maps Removal
  - Naming service backup/restore utility

Maps – Removal

- **Support updating naming service tables directly**
  - Transitioning to vendor-supplied
    - Group Maintenance
    - Host Maintenance
    - User Maintenance
- **Support Full Service Directory fields**
  - Extending User Maintenance
    - Add User Wizard
    - User Templates
- **Support Add / Remove / Modify commands**
  - Extending User Maintenance
- **Support Map Defaults**
  - User Maintenance’s “User Templates”

Maps – Backup Utility



- **Retain the capability to backup and restore naming service data**
  - Provide a naming service backup/restore utility
    - Modify SMC to manually call this utility
    - Configure Solaris Cron Utility to automatically call this utility

Roadmap

- **Solaris 9 Public Design Review**
  - JEDI 2.0 Requirements
  - Support for Solaris 9
  - Transition JEDI Tools to Role Based Access Control
  - Transition JEDI Tools to Solaris Management Console
  - Removing Dependency on JEDI Maps
  - Secure Shell
  - JASS Interface
  - Pluggable Authentication Modules
  - Flash Archive Support
  - Optional SASF for Solaris 9
  - Integration of ISS into JEDI 2.0 Baseline
  - Additional Recommendations

Roadmap – Secure Shell

- **Secure Shell (SSH)**
  - Secure Shell – Solaris 9
  - Secure Shell – Protocols 1 and 2
  - Secure Shell – Affects on RDIST and the Accept/Decline banner
  - Secure Shell – /etc/ssh/ssh_config
  - Secure Shell – Configuration GUI for SSH
  - Secure Shell – Support for Solaris 8

Secure Shell – Solaris 9

- **Secure Shell is provided with Solaris 9**

- **ssh (Secure Shell) is a program for logging into a remote machine and for executing commands on a remote machine**
  - Intended to replace rlogin and rsh
  - Provide secure encrypted communications between two untrusted hosts over an insecure network

- **ssh connects and logs into the specified hostname**
  - User must prove his or her identity to the remote machine
  - Two protocol methods
    - SSH Protocol 1
    - SSH Protocol 2
  - All communication with the remote command or shell is automatically encrypted

Secure Shell – Protocols 1 and 2

- **SSH Protocol 1**
  - RSA authentication protocol
  - Private key in $HOME/.ssh/identity
  - Public key in $HOME/.ssh/identity.pub
  - Keys reside in the user's home directory

- **SSH Protocol 2**
  - Public Key method similar to RSA in Protocol 1
    - DSA algorithm instead of patented RSA algorithm
  - Private key in $HOME/.ssh/id_dsa
  - Public key in $HOME/.ssh/authorized_keys
  - Keys reside in the user's home directory
  - Strong mechanism for ensuring integrity of the connection
    - Traffic encrypted using 3DES, Blowfish, CAST128 or Arcfour
    - Integrity ensured with hmac-sha1 or hmac-md5

Secure Shell - Affects on RDIST and the Accept/Decline banner

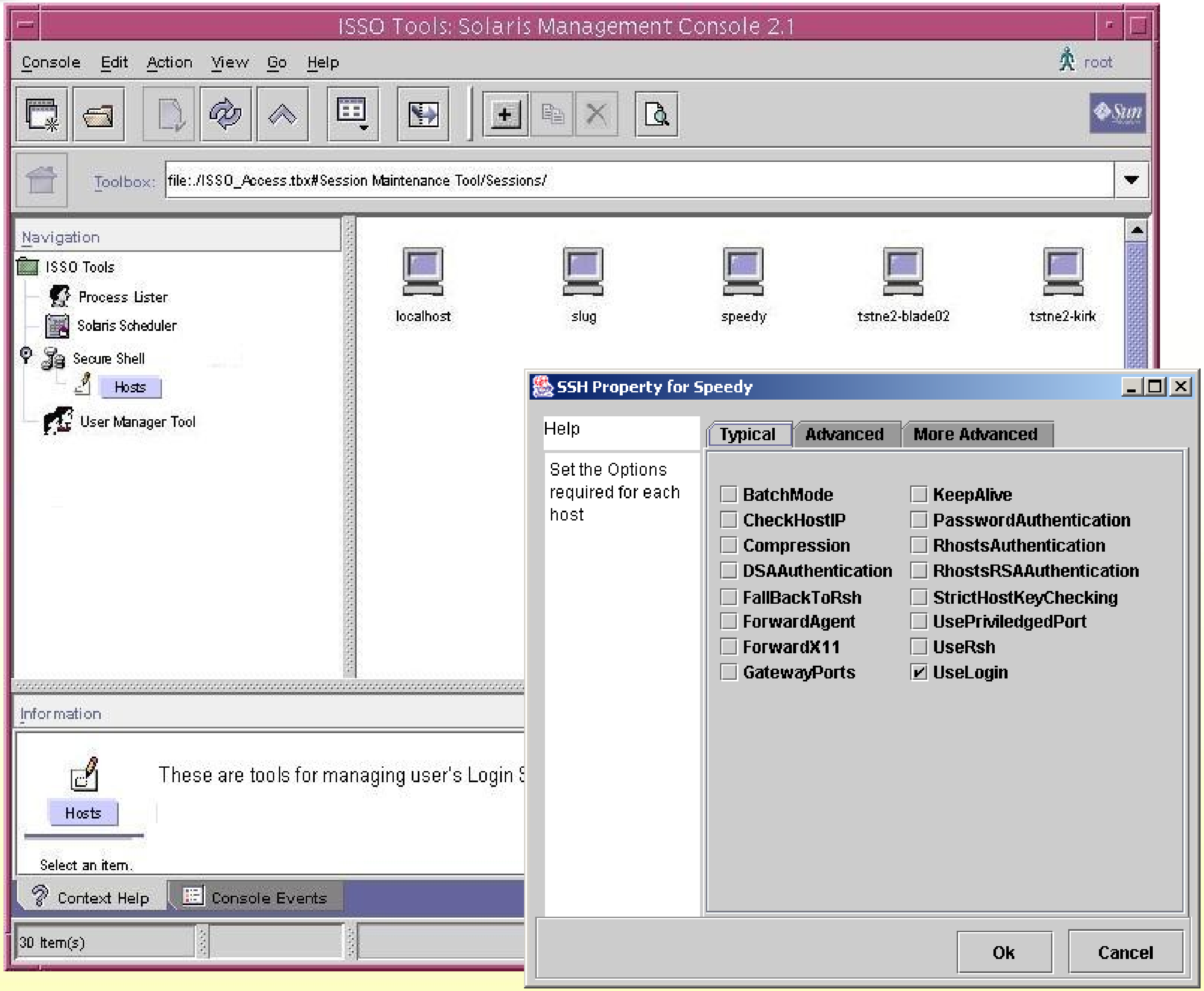
- **RDIST and Secure Shell**
  - Previous versions of RDIST utilized rsh for communications between hosts
  - RDIST for the Solaris 9 effort will utilize ssh
    - Changes will be made to RDIST for ssh
    - Legacy support for RDIST will be managed through the configuration of ssh
      - **UseRsh configuration parameter on a per legacy host basis will allow RDIST to communication using rsh**
      - **UseRsh parameter is stored in the ssh_config file**
      - **UseRsh parameter will be managed by the SSH_Config GUI**
- **Accept/Decline banner and Secure Shell**
  - Ssh for Solaris 9 supports PAM
  - Support for the Accept/Decline banner using PAM and the UseLogin SSH parameter stored in the ssh_config file
  - UseLogin parameter will be managed by the SSH-Config GUI

Secure Shell – /etc/ssh/ssh_config

- **/etc/ssh/ssh_config**
  - Contains the settings used by the Secure Shell software
  - Creating a GUI for managing this file
  - GUI will be a SMC Component

- **ssh_config GUI**
  - Help panel describing the options displayed
  - Reads the /etc/ssh/ssh_config file
  - If file is "empty", then the defaults will be shown in the GUI for the JEDI configuration
  - Cancel forgets the changes made to the file
  - OK saves the changes to the file

Secure Shell – Configuration GUI for SSH



Toolbox: file:./ISSO_Access.tbx#Session Maintenance Tool/Sessions/

- ISSO Tools
  - Process Lister
  - Solaris Scheduler
  - Secure Shell
    - Hosts
  - User Manager Tool

localhost
slug
speedy
tstne2-blade02
tstne2-kirk

These are tools for managing user's Login S

Hosts

Select an item.

30 Item(s)

SSH Property for Speedy

Help

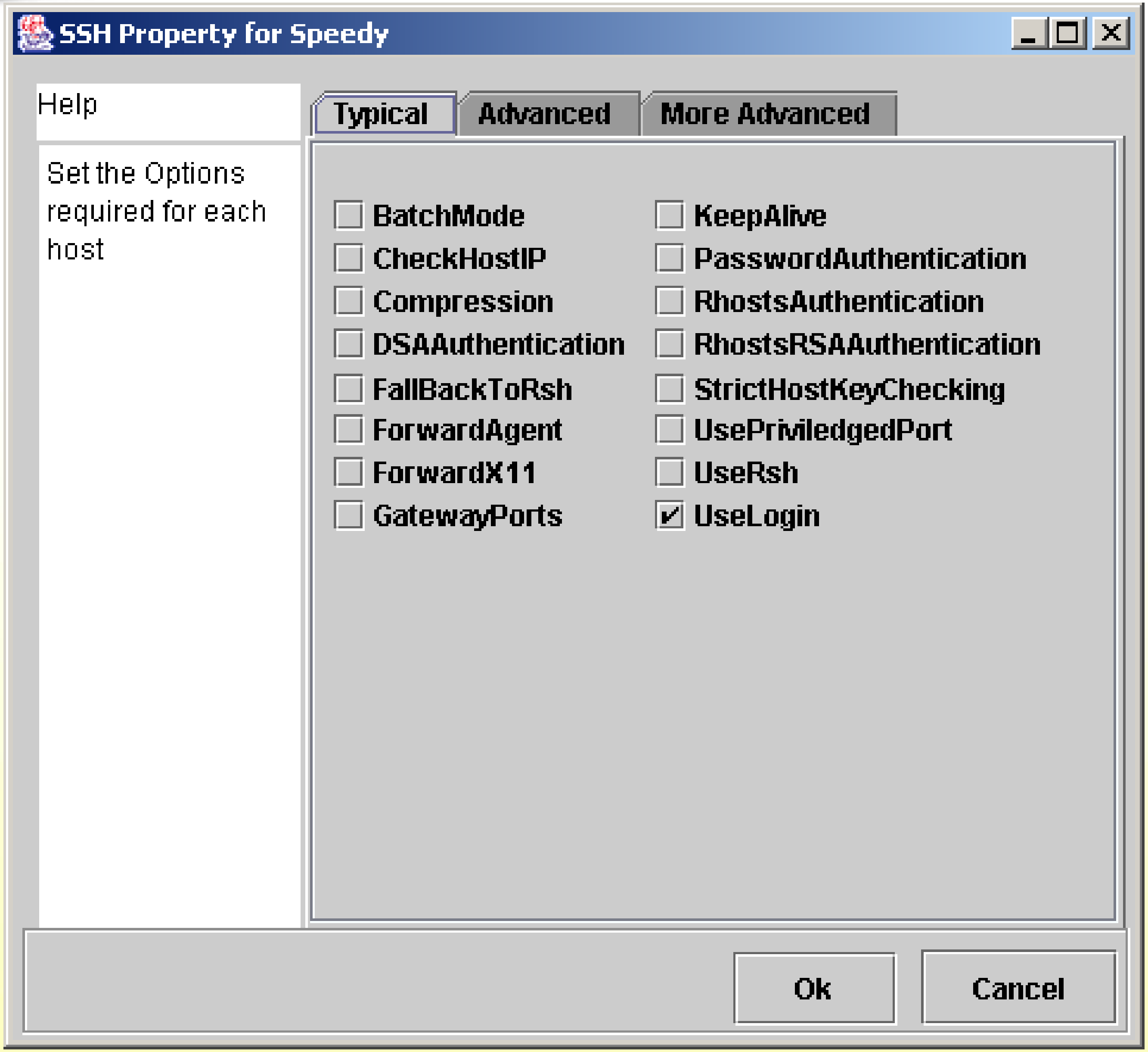
Set the Options required for each host

Typical | Advanced | More Advanced

□ BatchMode	□ KeepAlive
□ CheckHostIP	□ PasswordAuthentication
□ Compression	□ RhostsAuthentication
□ DSAAuthentication	□ RhostsRSAAuthentication
□ FallBackToRsh	□ StrictHostKeyChecking
□ ForwardAgent	□ UsePriviledgedPort
□ ForwardX11	□ UseRsh
□ GatewayPorts	☑ UseLogin

Ok
Cancel

Secure Shell – Configuration GUI for SSH (cont)



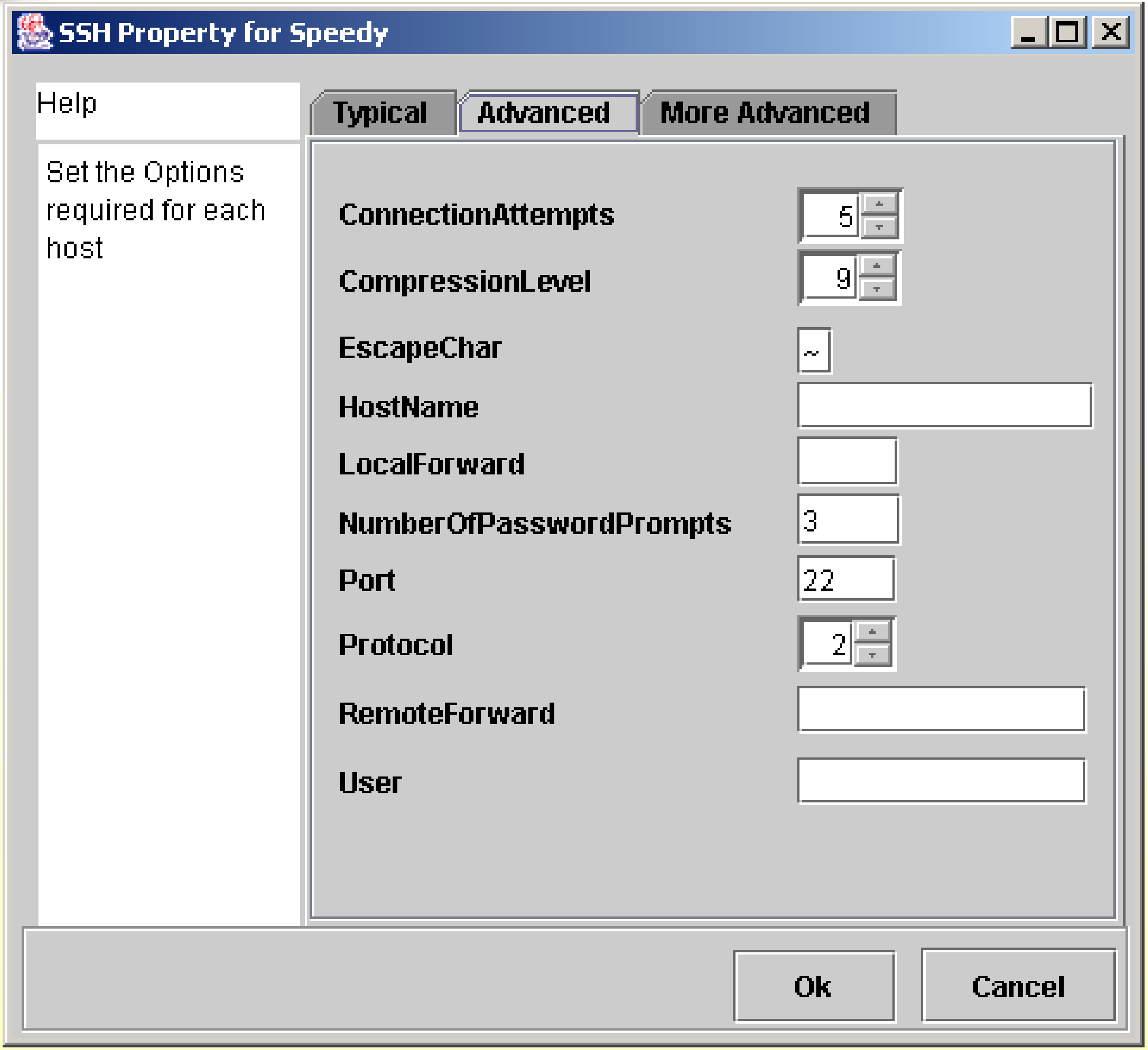
Help

Set the Options required for each host

☐ BatchMode
☐ CheckHostIP
☐ Compression
☐ DSAAuthentication
☐ FallBackToRsh
☐ ForwardAgent
☐ ForwardX11
☐ GatewayPorts

☐ KeepAlive
☐ PasswordAuthentication
☐ RhostsAuthentication
☐ RhostsRSAAuthentication
☐ StrictHostKeyChecking
☐ UsePriviledgedPort
☐ UseRsh
☑ UseLogin

Secure Shell – Configuration GUI for SSH (cont)



Set the Options required for each host

ConnectionAttempts 5

CompressionLevel 9

EscapeChar ~

HostName

LocalForward

NumberOfPasswordPrompts 3

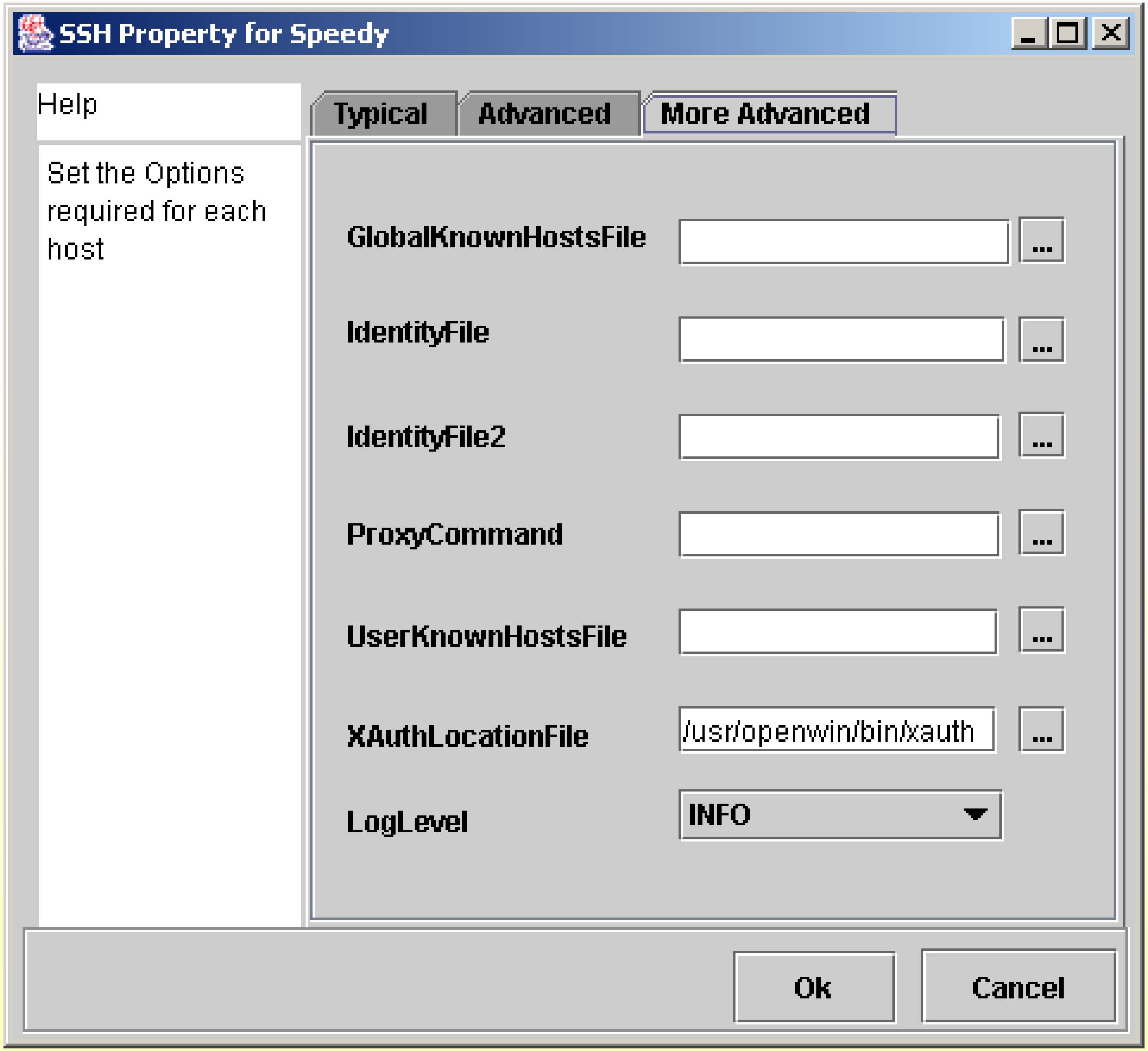
Port 22

Protocol 2

RemoteForward

User

Secure Shell – Configuration GUI for SSH (cont)



Set the Options required for each host

GlobalKnownHostsFile:

IdentityFile:

IdentityFile2:

ProxyCommand:

UserKnownHostsFile:

XAuthLocationFile: /usr/openwin/bin/xauth

LogLevel: INFO

Secure Shell – Support for Solaris 8

- **OpenSSH for Solaris 8**
  - Version 3.7.1p2
  - Software in Solaris pkgadd format
    - Download packages from sunfreeware.com
    - Security Fixes
      - Download new version from sunfreeware.com
      - Uninstall package(s) and Install in version(s)
  - Additional support packages
    - Openssl 0.9.7c
    - Zlib 1.1.4
    - Libgcc 3.3
    - Tcp Wrappers 7.6
    - Solaris 8 patch 112438-02 for /dev/random device
  - Provide needed packages on JEDI cdrom
  - Provide installation documentation

Roadmap

- **Solaris 9 Public Design Review**
  - JEDI 2.0 Requirements
  - Support for Solaris 9
  - Transition JEDI Tools to Role Based Access Control
  - Transition JEDI Tools to Solaris Management Console
  - ➡ Removing Dependency on JEDI Maps
  - Secure Shell
  - JASS Interface
  - Pluggable Authentication Modules
  - Flash Archive Support
  - Optional SASF for Solaris 9
  - Integration of ISS into JEDI 2.0 Baseline
  - Additional Recommendations

Roadmap – JASS Interface

- **JASS Interface**
  - JASS Interface – JEDI/OE Security
  - JASS Interface – GUI

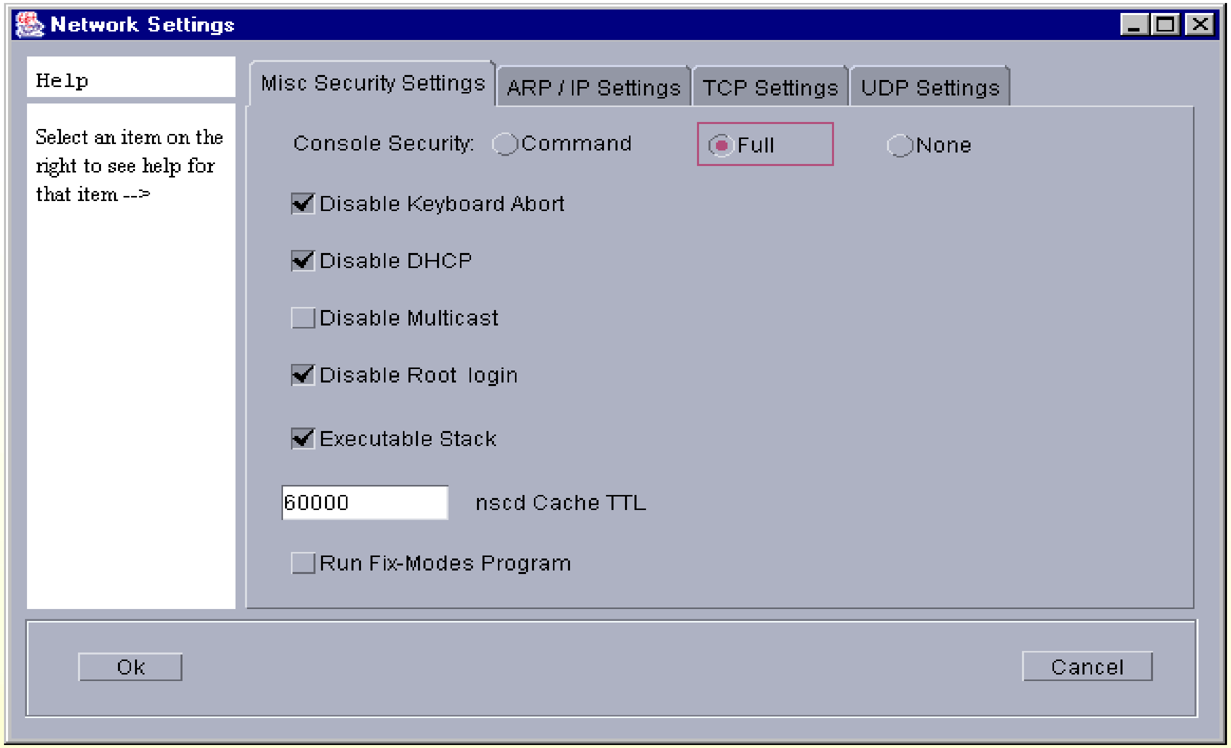
JASS Interface – JEDI/OE Security

- **JEDI 2.0 will use the JASS software as a platform for implementing**
  - Security guidelines
  - Templates
  - Best practices
    - Minimizing the Solaris 9 OE
    - Tightening network settings
- **JEDI 2.0 will make reasonable modifications to network parameters and protocols**
- **These settings will not compromise the functionality of JEDI 2.0 or site applications**

JASS Interface – JEDI/OE Security

- **JEDI 2.0 will install a JASS configuration file to implement the following**
  - Harden the File System
  - Ensure the latest Solaris OE is installed
  - Ensure the latest patches are installed
  - Ensure that Console Security is set correctly (EEPROM settings)
  - Ensure that Keyboard Abort is disabled
  - Ensure that Mount Options read-only, nosuid
    - In accordance with site policy
  - Ensure that Volume Management is Disabled
    - In accordance with site policy

JASS Interface – GUI



Help

Select an item on the right to see help for that item -->

Console Security: ○ Command ● Full ○ None

☑ Disable Keyboard Abort

☑ Disable DHCP

□ Disable Multicast

☑ Disable Root login

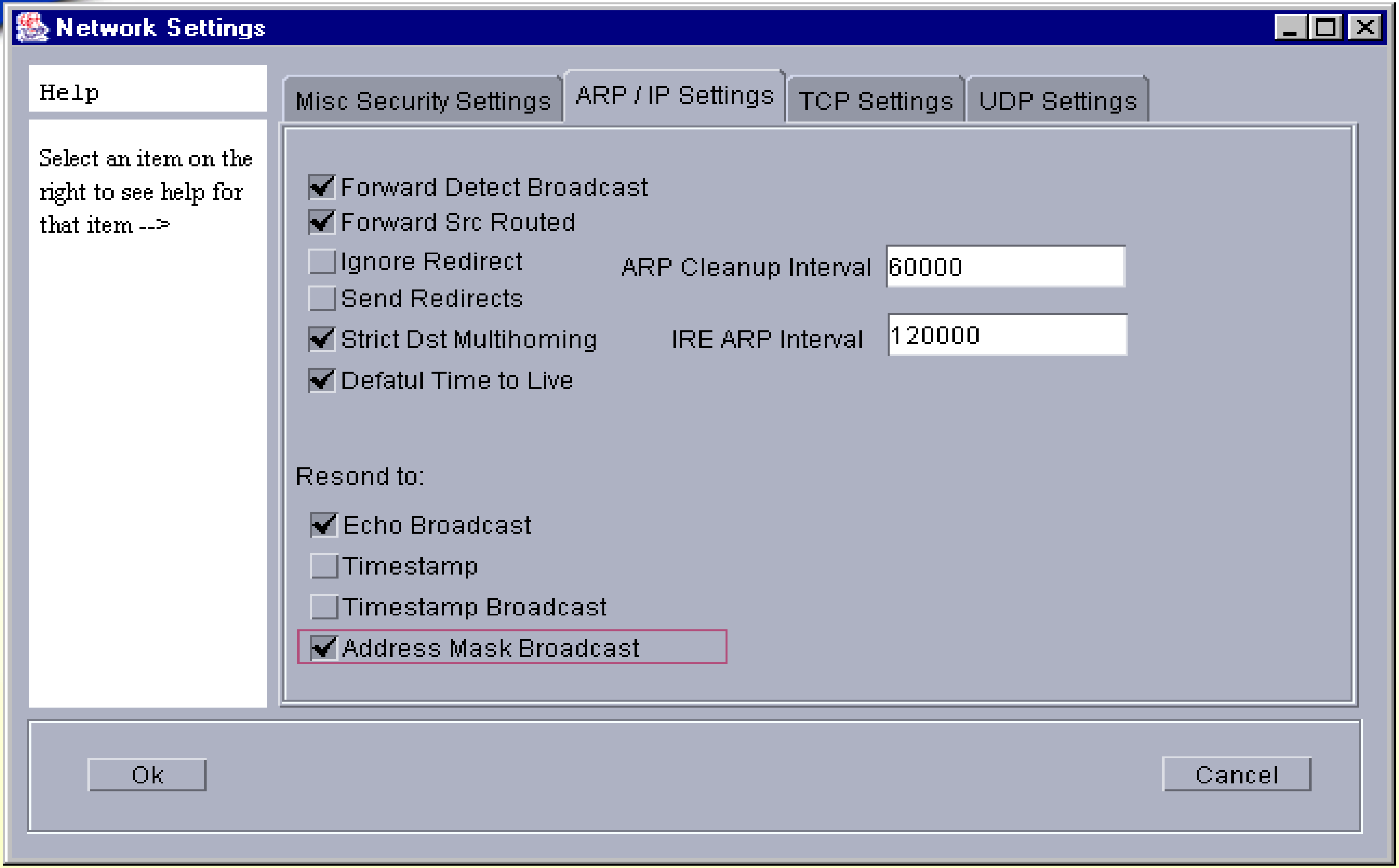
☑ Executable Stack

60000 nscd Cache TTL

□ Run Fix-Modes Program

- **JEDI 2.0 will provide a GUI front end for configuring workstation and network settings**
- **Security Settings will be broken down into two virtual groups**
  - Network settings
  - OS Settings

JASS Interface – GUI



Help

Select an item on the right to see help for that item -->

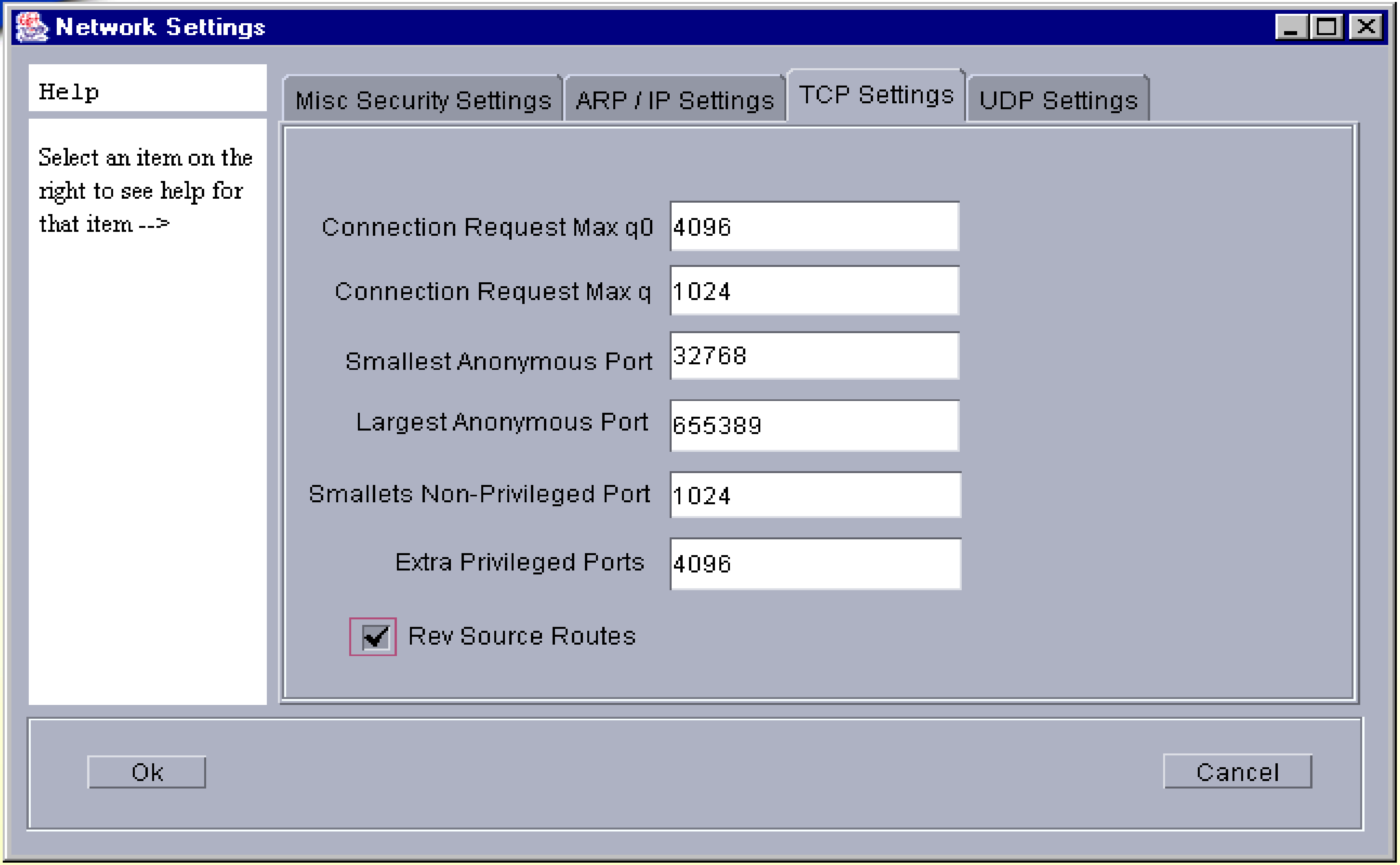
☑ Forward Detect Broadcast
☑ Forward Src Routed
□ Ignore Redirect
□ Send Redirects
☑ Strict Dst Multihoming
☑ Defatul Time to Live

ARP Cleanup Interval: 60000
IRE ARP Interval: 120000

Resond to:

☑ Echo Broadcast
□ Timestamp
□ Timestamp Broadcast
☑ Address Mask Broadcast

JASS Interface – GUI



Network Settings

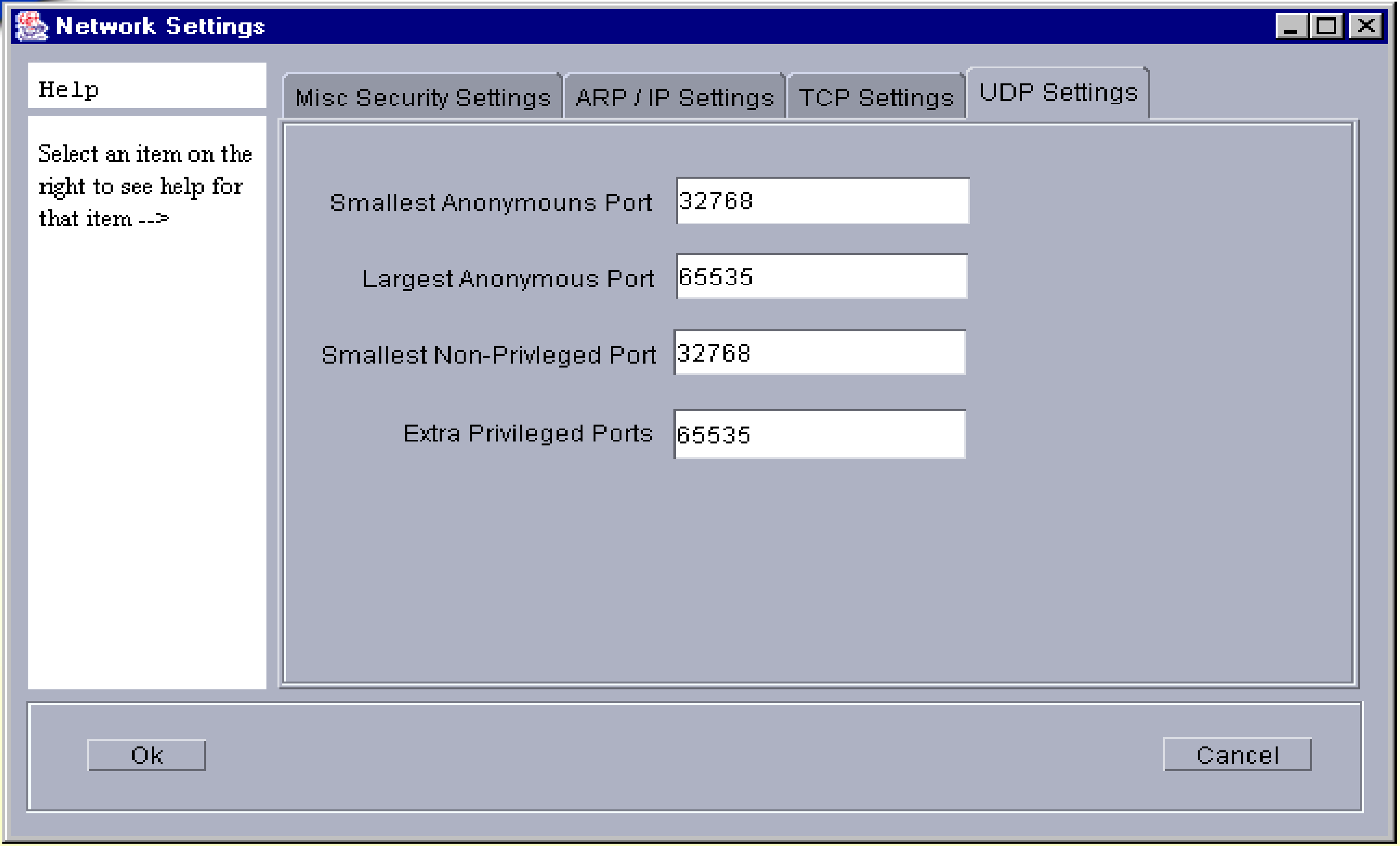
Help

Select an item on the right to see help for that item -->

Connection Request Max q0	4096
Connection Request Max q	1024
Smallest Anonymous Port	32768
Largest Anonymous Port	655389
Smallets Non-Privileged Port	1024
Extra Privileged Ports	4096

☑ Rev Source Routes

JASS Interface – GUI



Help

Select an item on the right to see help for that item -->

Smallest Anonymouns Port 32768

Largest Anonymous Port 65535

Smallest Non-Privleged Port 32768

Extra Privileged Ports 65535

Roadmap

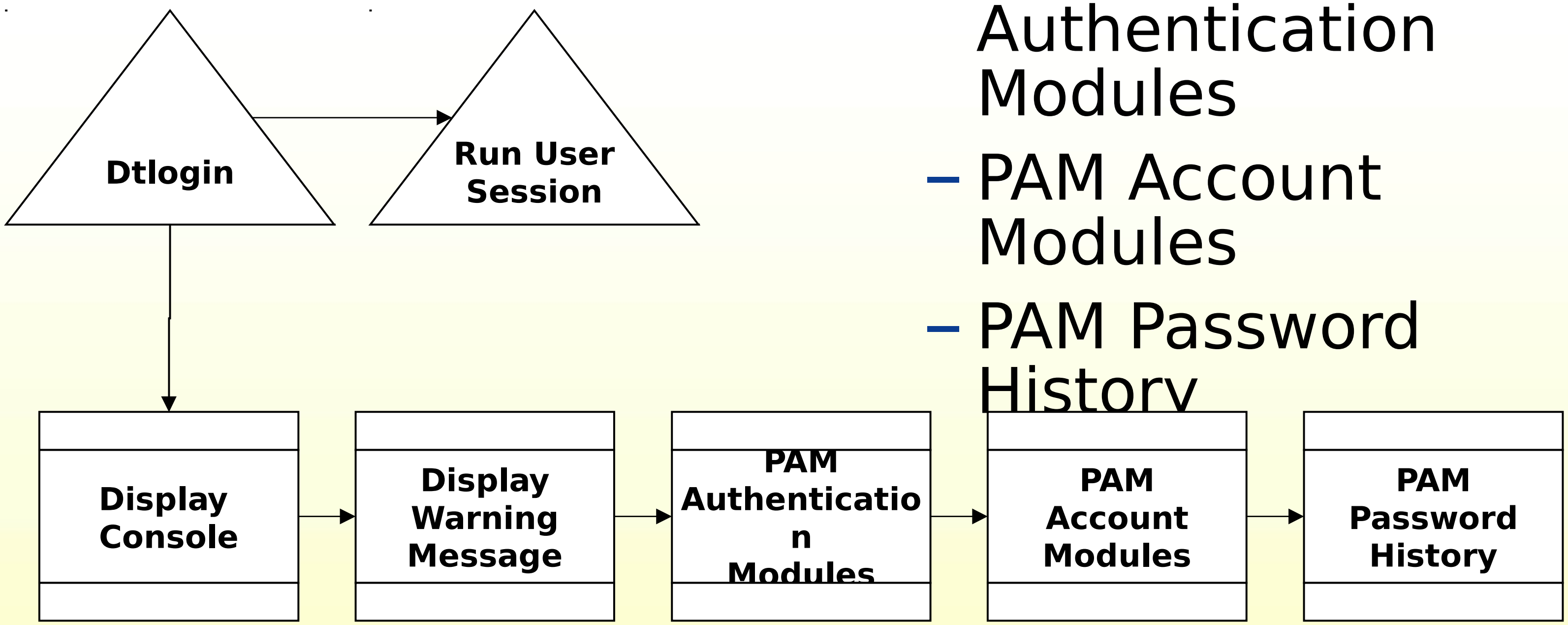
- **Solaris 9 Public Design Review**
  - JEDI 2.0 Requirements
  - Support for Solaris 9
  - Transition JEDI Tools to Role Based Access Control
  - Transition JEDI Tools to Solaris Management Console
  - Removing Dependency on JEDI Maps
  - Secure Shell
  - JASS Interface
  - Pluggable Authentication Modules
  - Flash Archive Support
  - Optional SASF for Solaris 9
  - Integration of ISS into JEDI 2.0 Baseline
  - Additional Recommendations

Roadmap – PAM

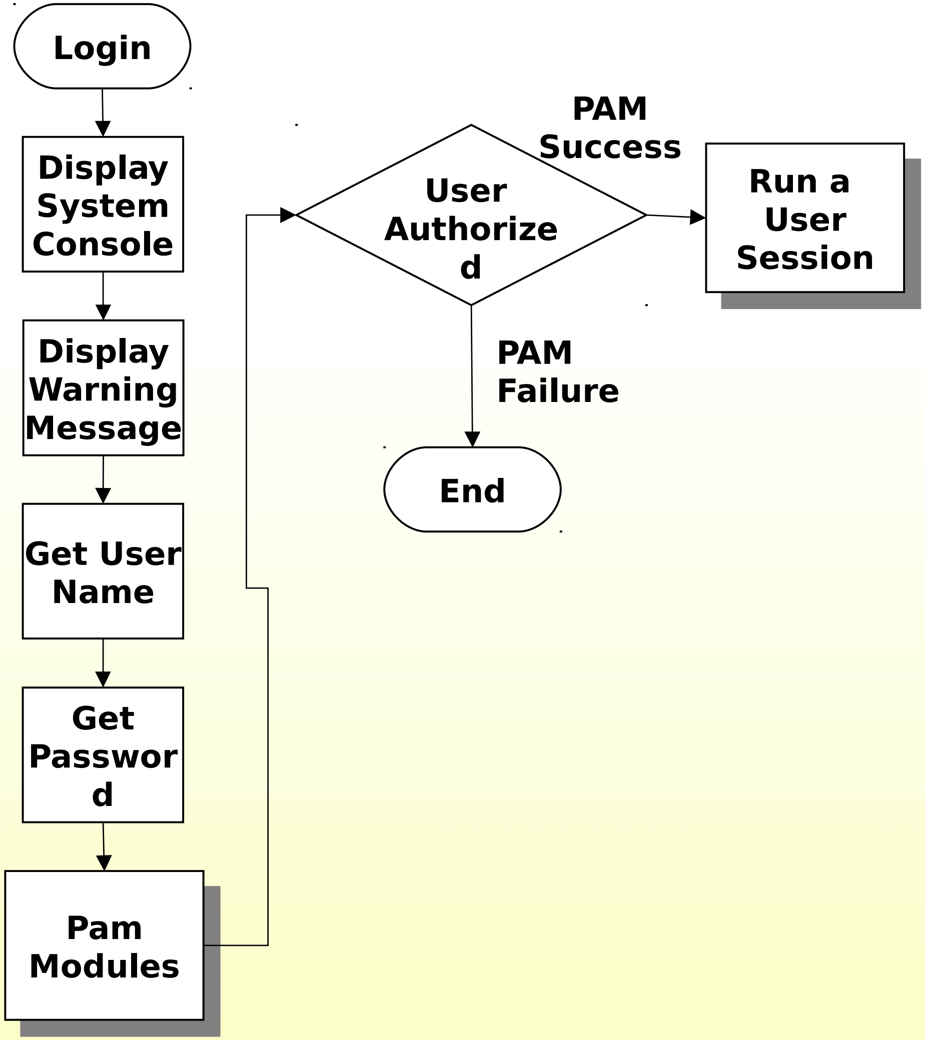
- **Pluggable Authentication Modules**
  - PAM – Incorporate New Native PAM
  - PAM – Login Functional Flow
  - PAM – Authentication Modules
  - PAM – Account Modules
  - PAM – Support for Password History
  - PAM – Password History Flow
  - PAM – Password History Updates – NIS
  - PAM – Password History Updates – NIS+/LDAP

PAM – Incorporate New Native PAM

- **In JEDI 2.0, PAM Modules will be implemented for**
  - PAM Authentication Modules
  - PAM Account Modules
  - PAM Password History

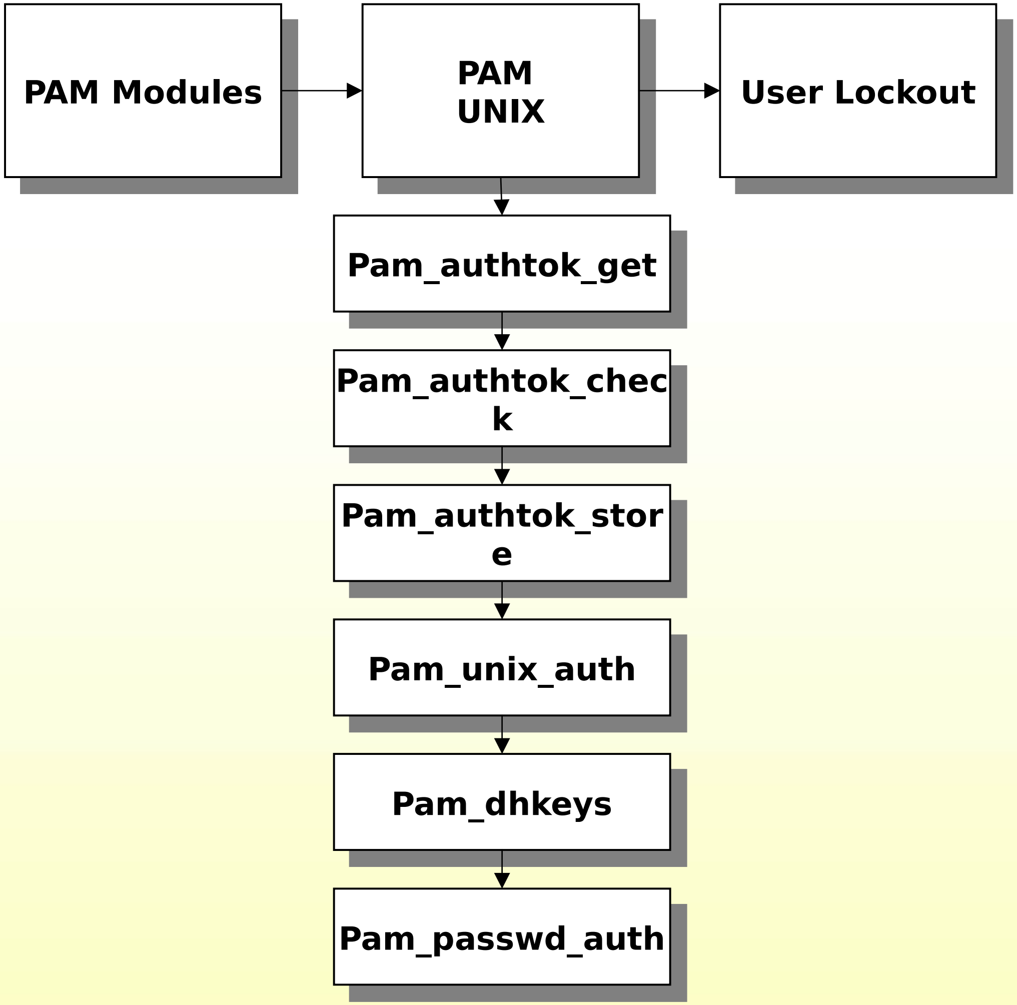


PAM – Login Functional Flow



- The user is prompted for the password during the login process
- The password is passed to the PAM Modules for authentication and verification
- If the password is correct and passes verification, the user is logged in

PAM – Authentication Modules



PAM Modules

PAM UNIX

User Lockout

Pam_authtok_get

Pam_authtok_check

Pam_authtok_store

Pam_unix_auth

Pam_dhkeys

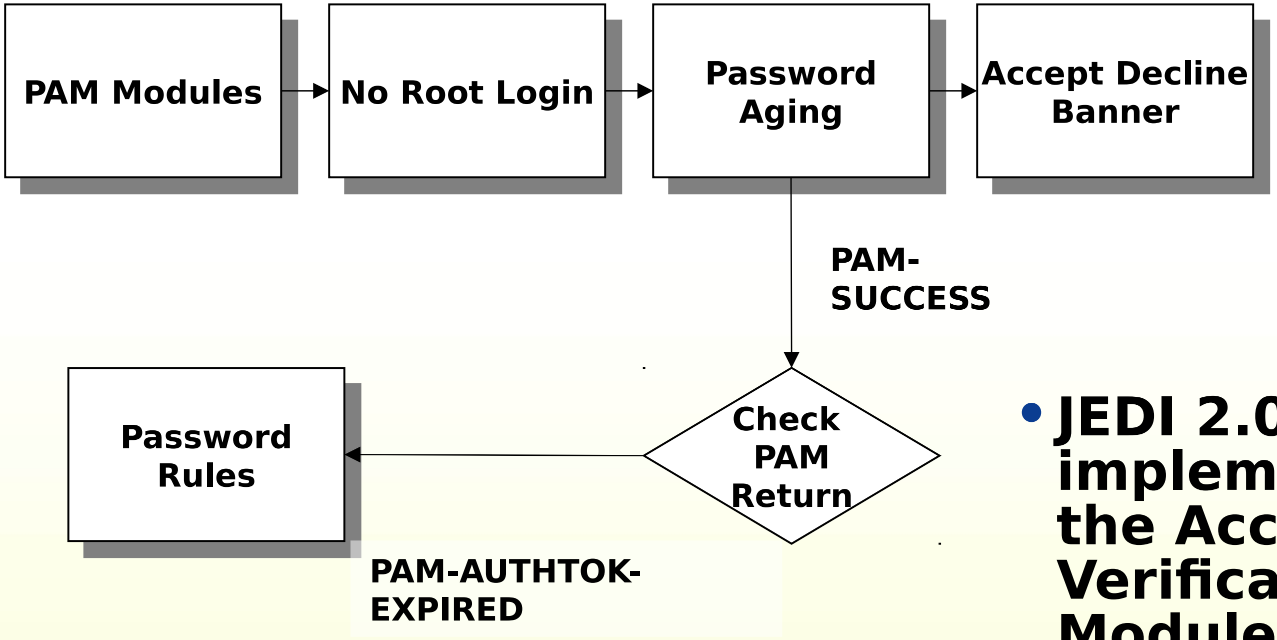
Pam_passwd_auth

- JEDI 2.0 will implement, as part of the Authentication Process, Modules for
  - Unix Authentication
  - User Lockout
- Under Solaris 9, The PAM Unix Modules are broken down into six modules
  - Pam_authtok_get
  - Pam_authtok_check
  - Pam_authtok_store
  - Pam_unix_auth
  - Pam_dhkeys
  - Pam_passwd_auth

PAM – Authentication Modules

- **Modules will return standard PAM return codes to indicate success or failure of the module**
  - PAM_AUTH_ERR
  - PAM_AUTHTOK_EXPIRED
  - PAM_SUCCESS
  - PAM_FAILURE
  - PAM_USER_UNKNOWN
- **The return codes are interpreted by the login process**
  - Dtlogin
  - FTP
  - Telnet

PAM – Account Modules



- **JEDI 2.0 will implement, as part of the Account Verification Process, Modules for**
  - No Root Login
  - Password Aging
  - Accept Decline Banner
  - Password Rules

PAM – Account Modules

- **Password Rules will be implemented as a PAM Module**
  - Solaris 9's PAM Password Module will be used to implement the following rules
    - Each password must have PASSLENGTH characters, where PASSLENGTH is defined in /etc/default/passwd
    - Each password must contain at least two alphabetic characters and at least one numeric or special character
    - Each password must differ from the user's login *name* and any reverse or circular shift of that login *name*
    - New passwords must differ from the old by at least three characters

PAM – Account Modules

- **The following rules will be implemented in PAM and will remain configurable**
  - Password must be at least 8 characters long
  - No repeating characters allowed as part of password
  - Password must be mixed case
  - Password must contain a special character
  - Login name not allowed as password
  - Reversed login name not allowed as password
  - First name not allowed as password
  - Reversed first name not allowed as password
  - Last name not allowed as password
  - Reversed last name not allowed as password
  - Office not allowed as password
  - Reversed office not allowed as password
  - Phone number not allowed as password
  - Reversed phone number not allowed as password

PAM – Account Modules

- **The following rules will be implemented in PAM and will remain configurable (continued)**
  - Initials not allowed as password
  - New password cannot be the same as previous password
  - User ID is not allowed as password or as part of password
  - Circular shift of username not allowed as password
  - Host name not allowed as password
  - Reversed host name not allowed as password
  - Domain name not allowed as password
  - Reversed domain name not allowed as password
  - Domained host name not allowed as password
  - Dictionary entries not allowed as password
  - Leading dictionary words not allowed as password
  - Trailing dictionary words not allowed as password
  - Password cannot have eight of the same characters

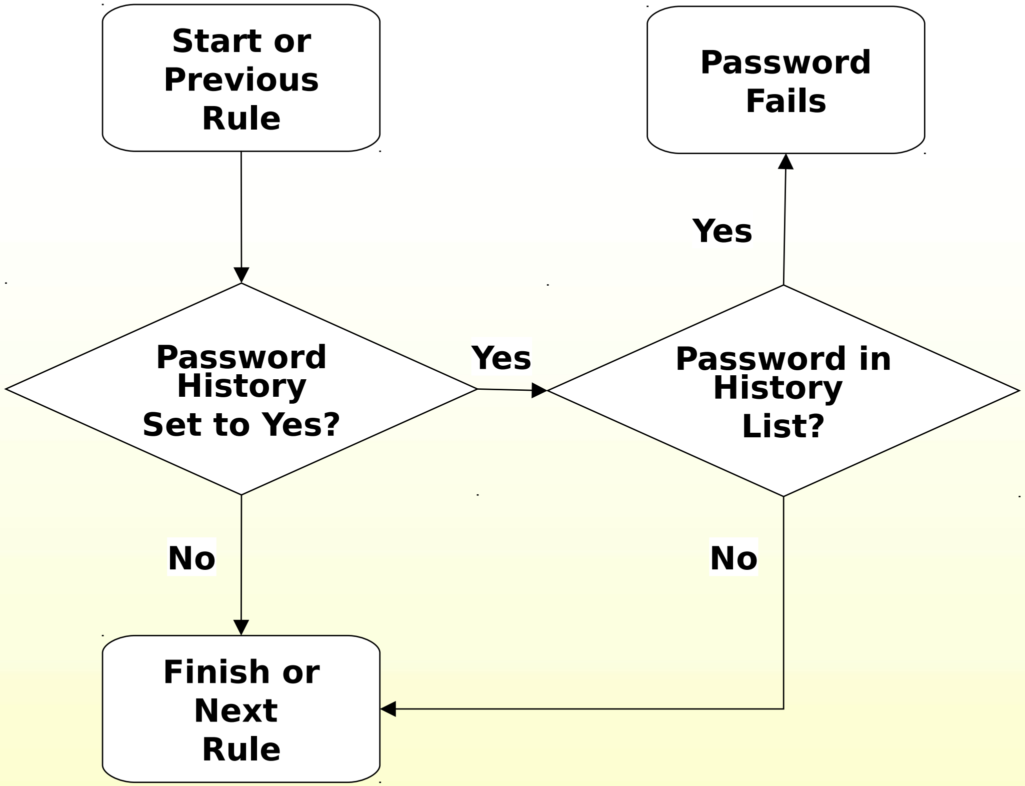
PAM – Support for Password History

- **JEDI 2.0 will use the Password History Object in LDAP**
  - The LDAP PasswordHistory has the following structure:
    - Binary, multiple values
  - Updated using the ldapmodify command
- **A password history table will be implemented in NIS+, NIS, and local files with the following format**
  - User:passwd1,passwd2, …, passwd*n*
  - Readable and writeable only by root
- **Created during the JEDI 2.0 Installation**
- **Invisible to the user**

PAM – Support for Password History

- **At installation time, the following attributes will be set in LDAP**
  - passwordHistory set to *on*
  - passwordInHistory set to *n*
    - Where *n* is the number of passwords to keep in the history
    - *N* defaults to 6
- **Two new variables will be added to the password.data**
  - PASSWORD_HISTORY
  - PASSWORD_IN_HISTORY
- **These variables will be set to the same values as collected in the installation software**

PAM – Password History Flow

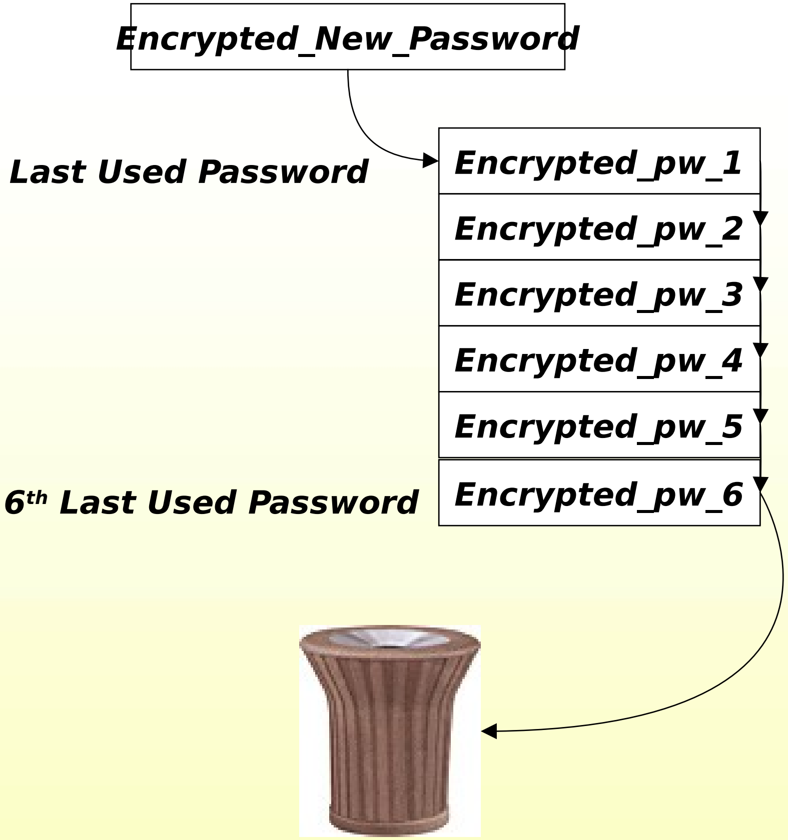


- Password History checking will be implemented as a rule in the passwd.data file
- Can be performed at any point in the password checking process
- Configurable by a trusted user
- Exceptions
  - Password will not be in the history if the list is blank

PAM – Password History Updates

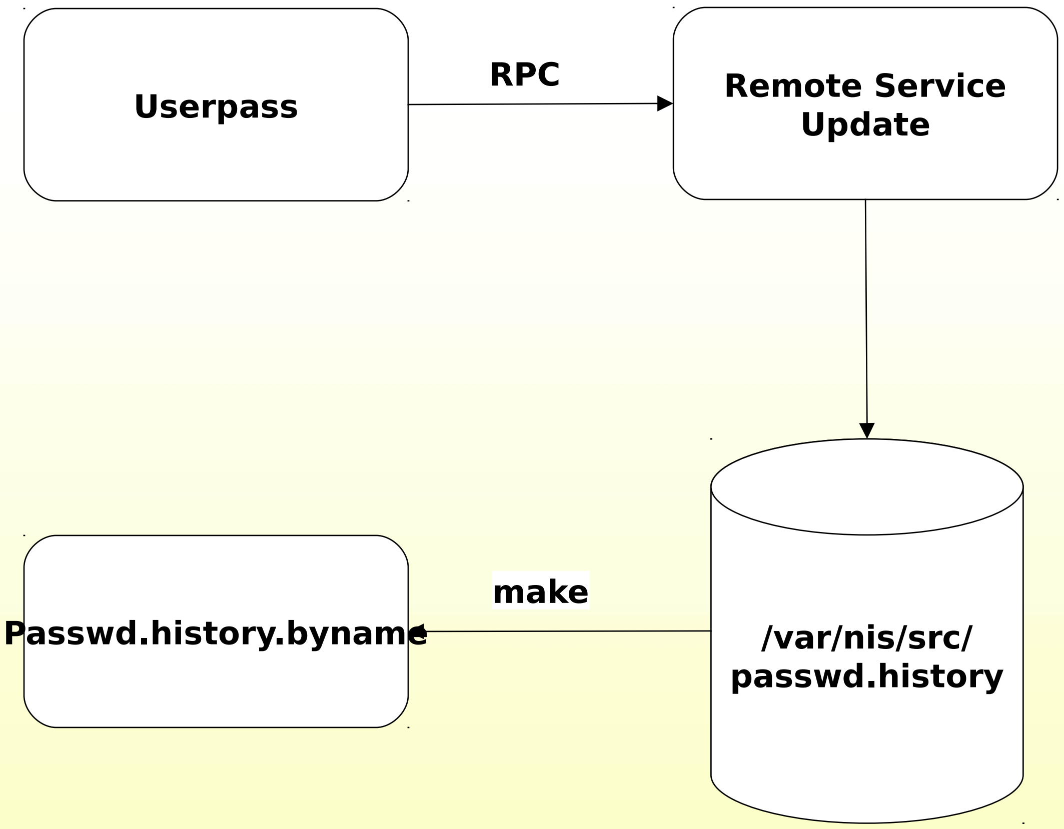
PASSORD_HISTORY=Yes

PASSORD_IN_HISTORY=6



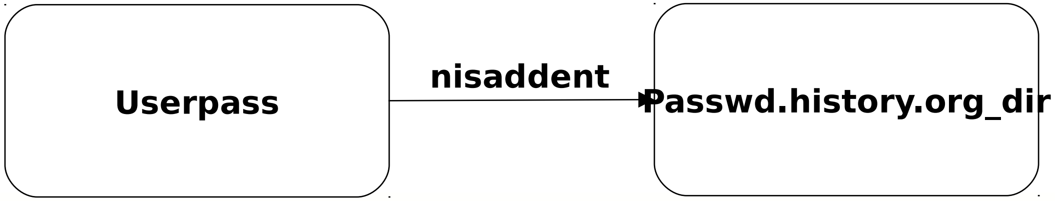
- Passwords are stored as encrypted values
- Userpass will read the PASSWORD_HISTORY variable
  - If set to Yes, Userpass will update the password history list
- Passwords are moved down the list
  - The last used password is moved to the number two slot
  - The 2nd last used password is moved to the number 3 slot, and so on
  - The nth password is discarded

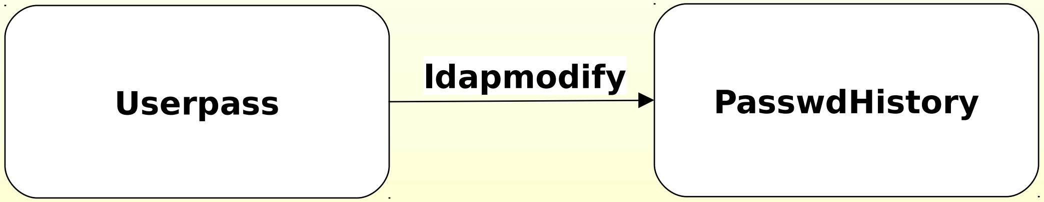
PAM – Password History Updates – NIS



- **NIS**
  - Userpass updates the passwd.history file
  - Make is executed updating the passwd.history table

PAM – Password History Updates – NIS+/LDAP





- **NIS+**
  - Userpass updates the passwd.history .org_dir table
    - Nisaddent commands
- **LDAP**
  - Userpass updates the PasswordHistory Object in LDAP
    - Ldapmodify commands

Roadmap

- **Solaris 9 Public Design Review**
  - Requirements
  - Support for Solaris 9
  - Transition JEDI Tools to Role Based Access Control
  - Transition JEDI Tools to Solaris Management Console
  - Removing Dependency on JEDI Maps
  - Secure Shell
  - JASS Interface
  - Pluggable Authentication Modules
  - Flash Archive Support
  - Optional SASF for Solaris 9
  - Integration of ISS into JEDI 2.0 Baseline
  - Additional Recommendations

Roadmap – Flash Archive Support

- **Flash Archive Support**
  - Flash Archive Support – Method
  - Flash Archive Support – Baseline

Flash Archive Support – Method

- **How will Flash archive be supported**
  - Jumpstart servers are created using the same methods for both normal jumpstart and flash archive support
  - Existing “Jumpstart Supplement” will be modified
    - **Section 2.1 “Solaris Jumpstart Overview” will be modified to introduce the concept of a “Flash Archive”**
    - **A new “Creating a Flash Archive” section will be added**

Flash Archive Support – Method

- Install and configure the system
- Create a Flash Archive
- Move the Archive to the Jumpstart Server
- Edit the rules file to use the archive
- Jumpstart the client system
- Test the system to determine if any of the COTS/GOTS software require an after-the-flash configuration

Flash Archive Support – Baseline

- **Flash Archive Directory Added**
  - Existing jumpstart directory structure will be modified to introduce a directory where newly created Flash Archives can be stored
- **Scripts**
  - Flash.begin and Flash.finish example scripts will be added
- **Rules**
  - Rules file will have an example rule added in support of a flash installation

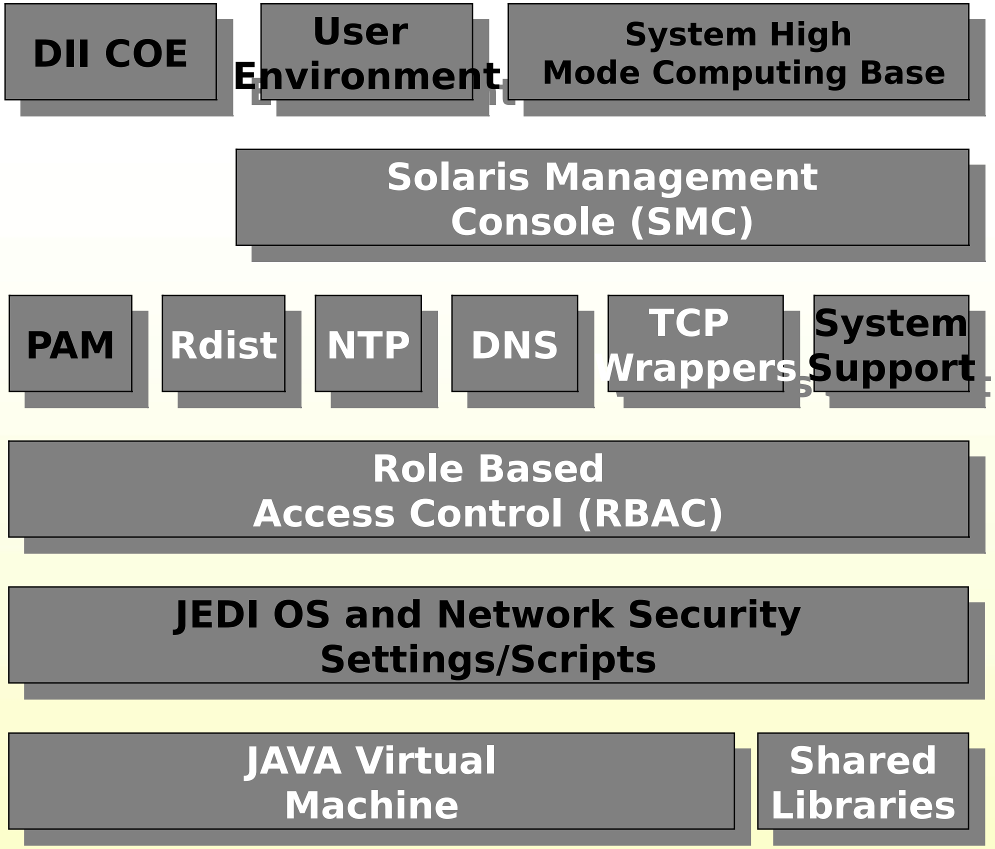
Roadmap

- **Solaris 9 Public Design Review**
  - Requirements
  - Support for Solaris 9
  - Transition JEDI Tools to Role Based Access Control
  - Transition JEDI Tools to Solaris Management Console
  - Removing Dependency on JEDI Maps
  - Secure Shell
  - JASS Interface
  - ➡ Pluggable Authentication Modules
  - Flash Archive Support
  - Optional SASF for Solaris 9
  - Integration of ISS into JEDI 2.0 Baseline
  - Additional Recommendations

Roadmap – Optional SASF for Solaris 9

- **Optional SASF for Solaris 9**
  - SASF – DII COE/JEDI Architecture
  - SASF – Modifications to DII COE
  - SASF – DII COE Installation Paths

SASF – DII COE/JEDI Architecture



DII COE

User Environment

System High Mode Computing Base

Solaris Management Console (SMC)

PAM

Rdist

NTP

DNS

TCP Wrappers

System Support

Role Based Access Control (RBAC)

JEDI OS and Network Security Settings/Scripts

JAVA Virtual Machine

Shared Libraries

- No runtime DII COE changes discovered to date
- Primary effort is dedicating to installing, verification, and testing

SASF – Modifications to DII COE

- **DII COE Kernel Modifications**
  - VerifySolarisVersion
    - Modify case statement to include Solaris 9 as an acceptable OS Version
  - CheckForFirstPatches
    - Modify case statement to include required patches for Solaris 9
- **ICSF Segment Modifications**
  - Process
    - Unbundle
    - Modify PostInstall for Solaris 9 installation
    - VerifySeg
    - MakeSeg (rebundle)
- **Issues**
  - Examining options for grouping the target segments into sets

SASF – ICSF Segments to be Modified

- **ICSF Segments**
  - Java Platform 2
  - Solaris Patch Update
  - JMTK Utilities Segment
  - JMTK SDBM
  - JMTK Analysis
  - Integrated Foundation Library
  - JMTK – Visualization
  - JMTK-V Map Data
  - Application Framework
  - Tactical Management System
  - TMS-Visualization
  - Universal Comms Processor
  - ICSF C4I

SASF - DII COE Installation Paths

- **Fresh Install**
  - Install Solaris 9
  - Install JEDI 2.0
  - Install Modified DII COE with Patch 9 (or latest available patch)
  - Install Modified ICSF Segments
- **Upgrade**
  - Existing System
    - Solaris 8, DII COE 4.2.0.5, JEDI 1.3, ICSF Segments
  - Patch DII COE to Patch 9
  - Upgrade Solaris 8→9
  - Upgrade JEDI 1.3→2.0

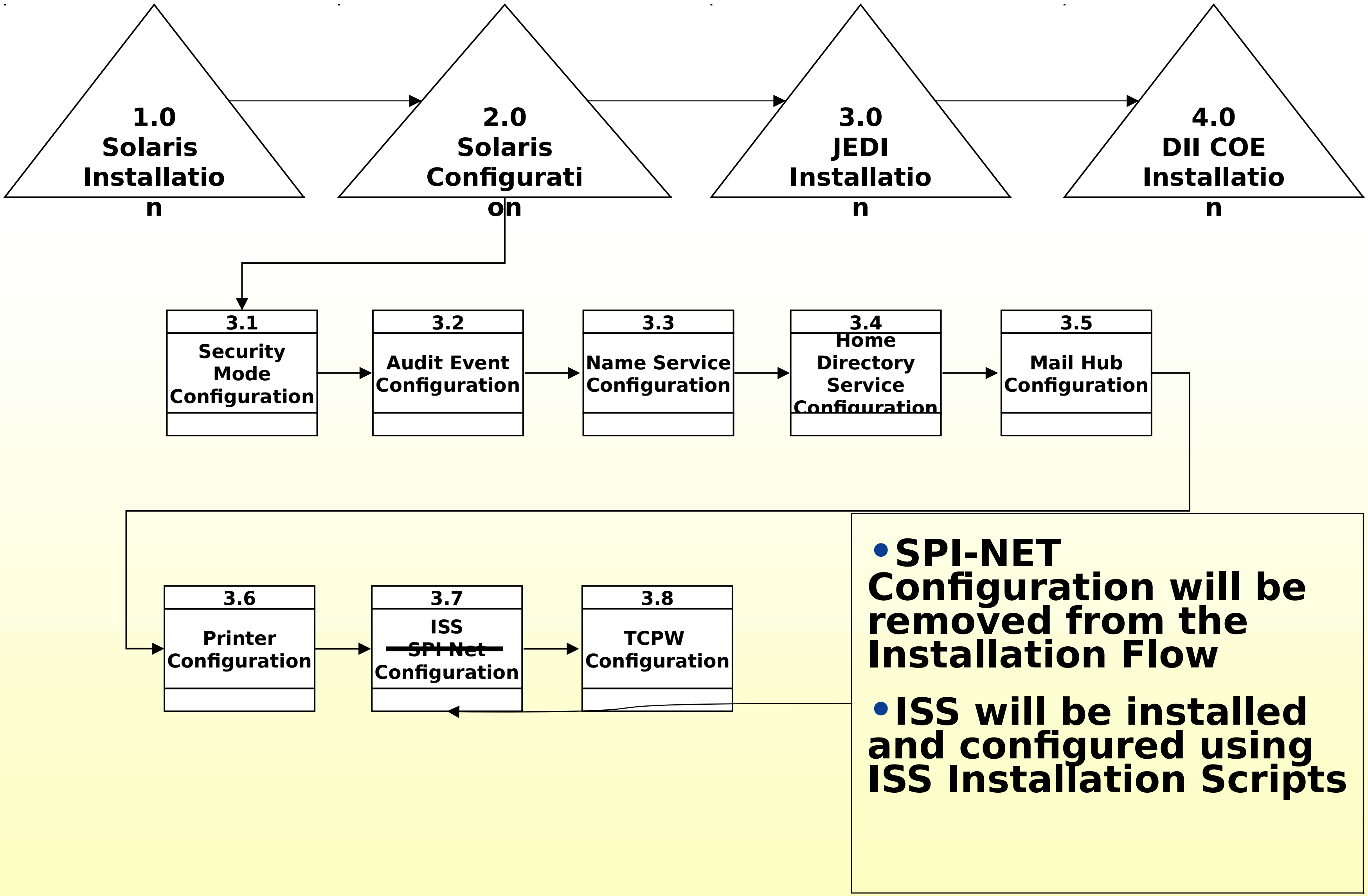
Roadmap

- **Solaris 9 Public Design Review**
  - Requirements
  - Support for Solaris 9
  - Transition JEDI Tools to Role Based Access Control
  - Transition JEDI Tools to Solaris Management Console
  - Removing Dependency on JEDI Maps
  - Secure Shell
  - JASS Interface
  - Pluggable Authentication Modules
  - Flash Archive Support
  - Optional SASF for Solaris 9
  - Integration of ISS into JEDI 2.0 Baseline
  - Additional Recommendations

Roadmap – Integration of ISS

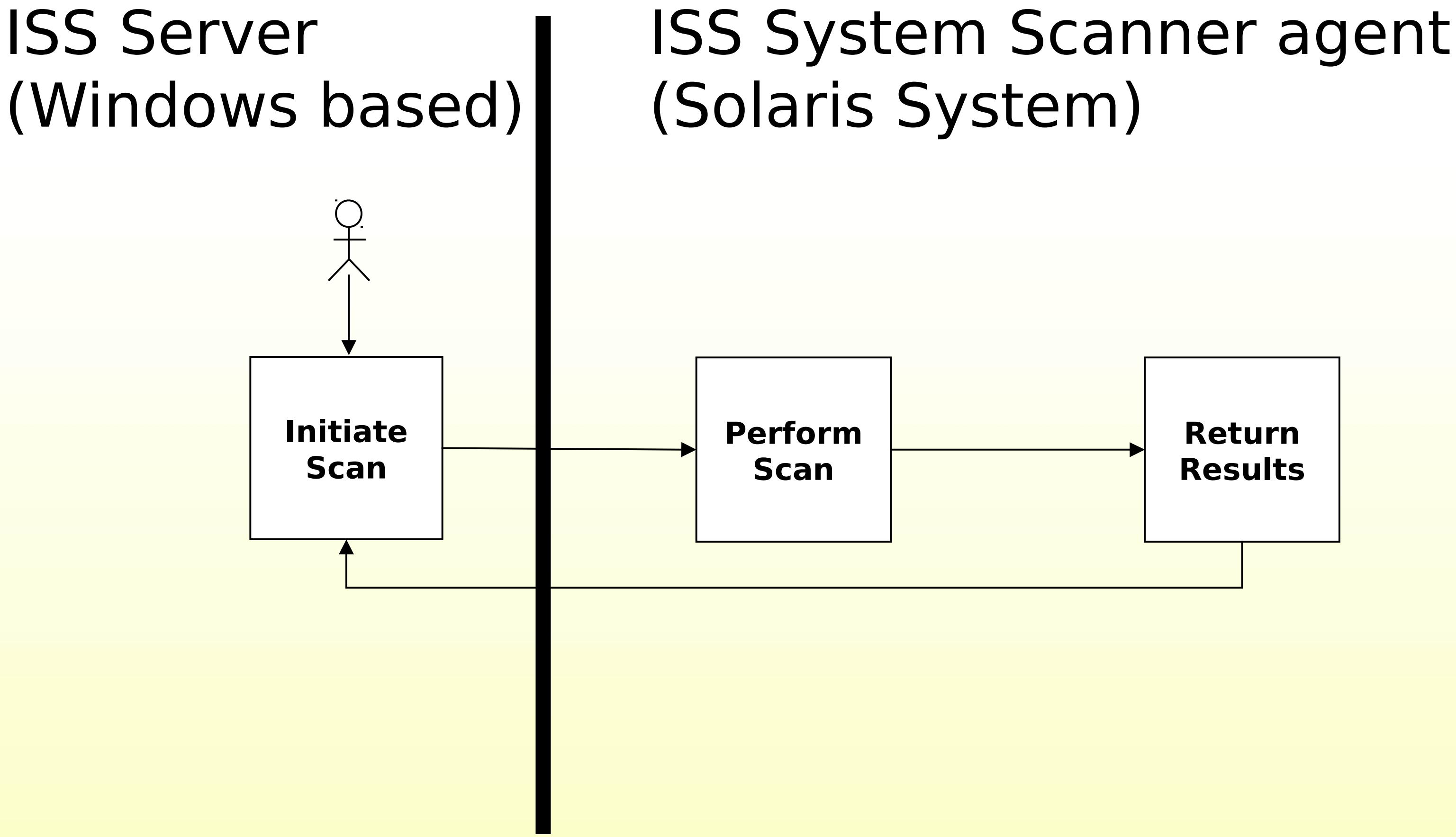
- **Integration of ISS into JEDI 2.0 Baseline**
  - ISS – Changes to Installation
  - ISS – Data Flow

ISS – Changes to Installation


1.0 Solaris Installation
2.0 Solaris Configuration
3.0 JEDI Installation
4.0 DII COE Installation
3.1 Security Mode Configuration
3.2 Audit Event Configuration
3.3 Name Service Configuration
3.4 Home Directory Service Configuration
3.5 Mail Hub Configuration
3.6 Printer Configuration
3.7 ISS ~~SPI-Net~~ Configuration
3.8 TCPW Configuration

- **SPI-NET Configuration will be removed from the Installation Flow**
- **ISS will be installed and configured using ISS Installation Scripts**

ISS – Data Flow



ISS Server
(Windows based)

ISS System Scanner agent
(Solaris System)

Initiate Scan

Perform Scan

Return Results

Roadmap

- **Solaris 9 Public Design Review**
  - Requirements
  - Support for Solaris 9
  - Transition JEDI Tools to Role Based Access Control
  - Transition JEDI Tools to Solaris Management Console
  - Removing Dependency on JEDI Maps
  - Secure Shell
  - Pluggable Authentication Modules
  - Flash Archive Support
  - Optional SASF for Solaris 9
  - Integration of ISS into JEDI 2.0 Baseline
  - Additional Recommendations

Roadmap – Additional Recommendations

- Remote Desktop
- Update Xautolock